UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS CIP-013-2, CIP-005-7, AND CIP-010-4 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

December 14, 2020

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS CIP-013-2, CIP-005-7, AND CIP-010-4 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] and Order No. 850,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval proposed Reliability Standards CIP-013-2 – Cyber Security – Supply Chain Risk Management, CIP-005-7 – Cyber Security – Electronic Security Perimeter(s), and CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments. The proposed Reliability Standards improve the reliability of the Bulk Electric System ("BES") and address the Commission's directive from Order No. 850 to develop modifications to include Electronic Access Control or Monitoring Systems ("EACMS")[5] associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. In addition, the proposed Reliability Standards address the NERC recommendation to address Physical Access Control Systems ("PACS") that provide physical access control to high

[1] 16 U.S.C. § 824o (2018).
[2] 18 C.F.R. § 39.5 (2020).
[3] *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018) [hereinafter Order No. 850].
[4] The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").
[5] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, http://www.nerc.com/files/Glossary_of_Terms.pdf.

and medium impact BES Cyber Systems.[6] NERC requests that the Commission approve the proposed Reliability Standards, provided in Exhibit A hereto, as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also requests approval of: (1) the associated Implementation Plan (Exhibit B); the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibit G); and the retirement of currently-effective Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3.

As required by Section 39.5(a) of the Commission's regulations,[7] this petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit H), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[8] (Exhibit C). The NERC Board of Trustees adopted the proposed Reliability Standards on November 5, 2020.

I. SUMMARY

In Order No. 850, the Commission approved Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 (the "Supply Chain Standards"). The Supply Chain Standards, which were developed in response to Order No. 829,[9] address cybersecurity risks associated with the supply chain for BES Cyber Systems. In approving the Supply Chain Standards, the Commission found that they addressed the following four objectives from Order No. 829: (1) software integrity and

---

[6] While the recommendation excluded the alarming and logging functions of PACS, the standard drafting team determined to include these functions of PACS in applicability. NERC, *NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, Docket No. RM17-13-000 (2019) [hereinafter NERC Supply Chain Report], at https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Supply%20Chain%20Report%20Filing.pdf.

[7] 18 C.F.R. § 39.5(a).

[8] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC 61,104 at PP 262, 321-37 (2006) [hereinafter Order No. 672], *order on reh'g*, Order No. 672-A, 114 FERC 61,328 (2006).

[9] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016) [hereinafter Order No. 829].

authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls.[10] The Commission further directed NERC to modify the Supply Chain Standards to include EACMS as applicable systems and file the modifications within 24 months of the effective date of Order No. 850.[11] Finally, the Commission accepted NERC's commitment to study certain categories of assets not currently the subject of the Supply Chain Standards, including PACS.[12] On May 28, 2019, NERC filed a report detailing NERC's assessment of supply chain risks as well as any recommended actions.[13] One such recommended action included modifications to the applicability of the Supply Chain Standards to include PACS.[14]

Consistent with Order No. 850 and the NERC Supply Chain Report, proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 (proposed "Supply Chain Standards") broaden supply chain risk management requirements to include EACMS and PACS as applicable systems. EACMS are devices that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter ("ESP") or BES Cyber Systems. As such, EACMS (e.g., firewalls or security information event management systems, among others) control or monitor electronic access to some of the most critical systems operating the BES. PACS are devices that control, alert, or log access to the Physical Security Perimeter ("PSP").[15] These devices help to manage physical access to defined areas that physically contain medium and high impact BES Cyber Systems. Similar to EACMS, PACS manage physical access to some of the most critical systems operating the BES. As such, including both EACMS and PACS as applicable systems in the Supply

[10] Order No. 850 at P 28. These four objectives were the subject of directives from Order No. 829.
[11] Order No. 850 at PP 30, 52.
[12] Order No. 850 at P 31.
[13] NERC Supply Chain Report.
[14] *Id.* at pp. 15-16.
[15] This does not include locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Chain Standards further enhances the reliability of the BES. The proposed Reliability Standards maintain the security objectives supported in the original version of the Supply Chain Standards while expanding protections for these additional applicable systems.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[16]

Lauren Perotti*
Senior Counsel
Marisa Hecht*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Howard Gugel*
Vice President, Engineering and Standards
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
howard.gugel@nerc.net

III. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[17] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[18] Section 215(d)(5) of the FPA authorizes

[16] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

[17] 16 U.S.C. § 824o.

[18] *Id.* § 824(b)(1).

the Commission to order the ERO to submit a new or modified Reliability Standard.[19] Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[20]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[21]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[22] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[23] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain criteria for approving Reliability

19 *Id.* § 824o(d)(5).
20 18 C.F.R. § 39.5(a).
21 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).
22 Order No. 672 at P 334.
23 The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

Standards.[24] The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the NERC Board of Trustees is required before NERC submits the Reliability Standard to the Commission for approval.

C. Order No. 850 Directive

The Supply Chain Standards originally were developed in response to directives in Order No. 829. In Order No. 829, the Commission directed NERC "to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with [BES] operations."[25]

In Order No. 850,[26] the Commission approved supply chain risk management Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 and directed additional modifications. Specifically, the Commission directed NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Standards.[27] The Commission declined to direct further detail, determining the following:

> [W]e leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risk. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.[28]

The Commission further noted that the standard drafting team could determine that a subset of EACMS may be appropriate for applicability of the supply chain risk management requirements,

---

24 ERO Certification Order at P 250.
25 Order No. 829 at P 2 (internal citations omitted).
26 Order No. 850.
27 *Id.*at PP 30, 51.
28 *Id.* at P 51.

citing the EACMS functions identified in Order No. 848.[29] The Commission directed NERC to file the modifications within 24 months of the effective date of Order No. 850.[30] In addition, the Commission accepted NERC's commitment to study certain categories of assets not currently subject to the Supply Chain Standards and directed NERC to file the final report, discussed below, with the Commission upon its completion.[31]

D. NERC Supply Chain Report

In adopting the Supply Chain Standards in August 2017, the NERC Board of Trustees issued resolutions[32] directing NERC to continue working with industry and vendors on supply chain issues, including further study of supply chain risks, among other activities. In carrying out the resolution to further study supply chain risk, NERC evaluated supply chain risks associated with certain categories of assets not subject to the Supply Chain Standards approved in Order No. 850. Based on this evaluation, NERC developed a report that included recommended actions to address those supply chain risks.[33] That report recommended the following standards modifications: (1) revise the Supply Chain Standards to address EACMS that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems; and (2) revise the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.[34] NERC filed the NERC Supply Chain Report with the Commission on May 28, 2019.[35]

---

29 *Id.* at P 55 (citing *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018)).

30 The effective date of Order No. 850 was December 26, 2018.

31 Order No. 850 at P 31.

32 The NERC Board of Trustees resolutions are available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

33 NERC Supply Chain Report.

34 *Id.* at pp. 9-11 and 15-16.

35 *Id.*

E. Development of the Proposed Reliability Standards

As further described in Exhibit H hereto, NERC initiated a Reliability Standard development project, Project 2019-03 Cyber Security Supply Chain Risks ("Project 2019-03"), and appointed a standard drafting team (Exhibit I) to address the Order No. 850 directive and the NERC Supply Chain Report recommendations. On January 27, 2020, NERC posted the initial drafts of proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 for a 45-day comment period and ballot. The initial ballot did not receive the requisite approval from the registered ballot body ("RBB"). After considering comments to the initial drafts, NERC posted second drafts of the proposed Reliability Standards for another 45-day comment period and ballot on May 5, 2020. The second drafts did not receive the requisite approval from the RBB. On July 28, 2020, NERC posted the third drafts of the proposed Reliability Standards after considering comments on the second drafts. The third drafts received the requisite approval from the RBB with an affirmative vote of 80.78 percent at 79.93 quorum. NERC conducted a 10-day final ballot for the proposed Reliability Standards, which received an affirmative vote of 76.76 percent at 83.56 quorum. The NERC Board of Trustees adopted the proposed Reliability Standards on November 5, 2020.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards enhance reliability by expanding the scope of protected equipment to include EACMS and PACS, thereby addressing the Commission's directive in Order No. 850 and the NERC Supply Chain Report recommendations, and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The proposed revisions incorporate EACMS and PACS as applicable systems in the Supply Chain Standards through language that accounts for the unique role played by these systems, particularly by EACMS. The following section discusses the revisions to the standards:

- the revised Requirement R1 in proposed Reliability Standard CIP-013-2 (Subsection A)
- the new Requirement R3 in proposed Reliability Standard CIP-005-7 (Subsection B); and
- the revised applicability in proposed Reliability Standard CIP-010-4 (Subsection C).

This section concludes with a discussion of the enforceability of the proposed Reliability Standards (Subsection D).

A. Proposed Reliability Standard CIP-013-2

Proposed Reliability Standard CIP-013-2 requires Responsible Entities to consider and address cyber security risks from vendor products or services during planning for the procurement of BES Cyber Systems as well as EACMS and PACS. Proposed Reliability Standard CIP-013-2 includes three requirements: (1) Requirement R1 requires a Responsible Entity to develop documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and includes requirement parts detailing the processes to include in the plan; (2) Requirement R2 requires Responsible Entities to implement the plan(s); and (3) Requirement R3 requires review and CIP Senior Manager, or delegate, approval of the plan(s) at least once every 15 calendar months.

Proposed Reliability Standard CIP-013-2 only includes modifications to Requirement R1, although the entire standard applies to EACMS and PACS. The modifications are shown in blackline below:

> **R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems **and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)**. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
>
> **1.1.** One or more process(es) used in planning for the procurement of BES Cyber Systems **and their associated EACMS and PACS** to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and

installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems**, and their associated EACMS and PACS,** that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System **and their associated EACMS and PACS**; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated ~~Interactive Remote Access, and (ii) system-to-system~~ remote access ~~with a vendor(s)~~.

The revisions to Requirement R1 require Responsible Entities to add EACMS and PACS associated with medium and high impact BES Cyber Systems to documented supply chain cyber security risk management plans. These requirements address risks during the planning stage when procuring BES Cyber Systems, EACMS, and PACS. The revisions to Requirement R1 now require that Responsible Entities: (1) adequately consider security risks when planning for EACMS and PACS associated with high and medium impact BES Cyber Systems (Part 1.1); and (2) address relevant security concepts in future contracts for EACMS and PACS associated with high and medium impact BES Cyber Systems (Part 1.2).

Additionally, revised Part 1.2.6 clarifies requirements surrounding remote access to accommodate applicability to EACMS and PACS by removing the term Interactive Remote Access and the phrase "system-to-system." This revision helps to coordinate with language in new Requirement R3 in proposed Reliability Standard CIP-005-7, as more fully described in Section IV.B. below, and continues to work in tandem with proposed CIP-005-7, Requirement R2, Parts 2.4 and 2.5. The revised requirement still achieves the objective of providing for vendor remote access protections as directed in Order No. 829.[36]

B. Proposed Reliability Standard CIP-005-7

Proposed Reliability Standard CIP-005-7 includes requirement parts that address supply chain risk management in the operational phase. The existing Parts 2.4 and 2.5 include remote access controls for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. Proposed new Requirement R3, which includes new Parts 3.1 and 3.2, addresses remote access controls for EACMS and PACS associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. Proposed Requirement R3 reads as follows:

> **R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

Within Requirement R3, CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS includes two new requirement parts. Proposed Parts 3.1 and 3.2 apply to EACMS and PACS associated with: (1) high impact BES Cyber Systems; and (2) medium impact

[36] Order No. 829 at P 51.

BES Cyber Systems with External Routable Connectivity. Proposed Parts 3.1 and 3.2 provide as follows:

> **3.1** Have one or more method(s) to determine authenticated vendor-initiated remote connections.
>
> **3.2** Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.

These new requirement parts work in tandem with Requirement R1, Part 1.2.6 of proposed Reliability Standard CIP-013-2 (discussed in Section IV.A above) to address vendor remote access and are similar to CIP-005-7, Requirement R2, Parts 2.4 and 2.5, which address remote access controls in the operational phase for medium and high impact BES Cyber Systems. However, based on the functions EACMS perform, there are some key distinctions in Parts 3.1 and 3.2 compared to Parts 2.4 and 2.5, as described below.

EACMS perform several monitoring and managing functions, including acting as an Intermediate System. Under Requirement R2, Part 2.1, Responsible Entities must use an Intermediate System, which is a type of EACMS, for Interactive Remote Access to a high impact BES Cyber System and a medium impact BES Cyber System with External Routable Connectivity. In performing this function, the EACMS is controlling the remote access to the BES Cyber System. As such, those vendors seeking to use Interactive Remote Access with an applicable BES Cyber System would first need to be authorized by the EACMS – in this case, an Intermediate System. In performing this role, the EACMS appropriately would deny access to a vendor that is not authorized. The standard drafting team did not want this normal function of an EACMS to be considered a "session" for purposes of applying the supply chain risk management protections simply because the vendor interacted with the EACMS but did not gain access to the BES Cyber System. Accordingly, the term "connection" describes when an authorized vendor is granted

access by the EACMS. Parts 3.1 and 3.2 use the terms "connection" instead of "session," which is used in Parts 2.4 and 2.5.

Likewise, Parts 3.1 and 3.2 do not use the terms "Interactive Remote Access" or "system-to-system remote access" (as used in Parts 2.4 and 2.5) because the standard drafting team determined the term "access" could be ambiguous when applied to EACMS. Based on comments received, the standard drafting team identified that "access" could be interpreted to include the Intermediate System function scenario described above, where a vendor interacts with an EACMS but is denied access to the BES Cyber System due to lack of authorization. As a result, the standard drafting team did not carry over the references to "Interactive Remote Access" and "system-to-system remote access" from Parts 2.4 and 2.5 in CIP-005-7, Requirement R3, Parts 3.1 and 3.2.

Finally, the term "authenticated" was used to describe access that has already been established by a user. As an EACMS can perform an authenticating function, the standard drafting team again determined this better described those connections that had already been established (subject to Requirement R3) versus those connections that were trying to be established (not subject to Requirement R3). Finally, the standard drafting team chose to use "terminate" combined with "control the ability to reconnect" instead of "disable" (which is used in Part 2.5) in Part 3.2 because it more granularly described the methods entities should employ when managing access to EACMS.

C. Proposed Reliability Standard CIP-010-4

Proposed Reliability Standard CIP-010-4 includes revisions to the applicability in Requirement R1, Part 1.6. The proposed revisions expand applicability to: (1) EACMS associated with high and medium impact BES Cyber Systems; and (2) PACS associated with high and medium impact BES Cyber Systems. As such, Requirement R1, Part 1.6 of proposed Reliability Standard CIP-010-4, whose requirement language remains unchanged from CIP-010-3, includes

the following as applicable to high and medium impact BES Cyber Systems and their associated EACMS and PACS:

> **1.6** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
>
> 1.6.1. Verify the identity of the software source; and
>
> 1.6.2. Verify the integrity of the software obtained from the software source.

In its petition for approval of CIP-013-1, CIP-005-6, and CIP-010-3, NERC explained that:

> Essentially, Part 1.6 provides that prior to installing software that changes the established baseline configuration for (1) operating system(s) (including version) or firmware where no independent operating system exists (Part 1.1.1), (2) any commercially available or open-source application software (including version) intentionally installed (Part 1.1.2), or (3) any custom software installed (Part 1.1.3), Responsible Entities must verify the identity of the software source and the integrity of the software obtained by the software sources, when methods are available to do so…. These steps, as the Commission stated in Order No. 829, help "reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System."[37]

As revised, the standard will now help reduce the risk of an attacker exploiting this process for EACMS and PACS by requiring Responsible Entities to apply these protections to EACMS and PACS.

Similar to Parts 2.4 and 2.5 and Requirement R3 of proposed CIP-005-7, proposed CIP-010-4, Requirement R1, Part 1.6 complements the procurement requirements in CIP-013-2 by requiring Responsible Entities to verify software integrity and authenticity for EACMS and PACS in the operational phase.

---

[37] *Petition of NERC for Approval of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Docket No. RM17-13-000, p. 33 (Sep. 26, 2017) (citing Order No. 829 at P 49).

D. Other Modifications

The proposed Reliability Standards also contain a number of minor modifications to align the standards with revisions to other standards or initiatives in other areas. These changes are shown in redline in Exhibit A and are summarized below.

The Interchange Coordinator or Interchange Authority is removed from the Applicability section of proposed Reliability Standards CIP-005-7 and CIP-010-4. This revision is consistent with FERC-approved changes to the NERC Compliance Registry under the risk-based registration initiative.[38]

Additionally, the proposed Reliability Standards include other minor modifications to the non-enforceable sections of the standard.

E. Enforceability of Proposed Reliability Standards

The proposed Reliability Standards also include measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[39] Additionally, the proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment. Exhibit G provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

---

[38] *N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,213 (2015) (approving removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

[39] Order No. 672 at P 327.

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standards to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan provides that the proposed Reliability Standards shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the Commission's order approving the proposed Reliability Standard. The 18-month implementation period is designed to afford Responsible Entities sufficient time to develop and implement their supply chain cybersecurity risk management plans incorporating EACMS and PACS associated with high and medium BES Cyber Systems according to proposed Reliability Standard CIP-013-2, implement the new requirement in proposed Reliability Standard CIP-005-7 for EACMS and PACS associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, and implement the controls in proposed Reliability Standard CIP-010-4, Requirement R1, Part 1.6 for EACMS and PACS.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve:

- proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4, and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B; and
- the retirement of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3, effective as proposed herein.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: December 14, 2020

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A

The Proposed Reliability Standards Addressing
Supply Chain Cybersecurity Risk Management

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-1

Proposed Reliability Standard CIP-013-2
Clean

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-1

Proposed Reliability Standard CIP-013-2
Redline to Last Approved (CIP-013-1)

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-~~1~~2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

~~**4.2.2.1.** All BES Facilities.~~

4.2.3. Exemptions: The following are exempt from Standard CIP-013-~~1~~2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002~~ 5,~~ or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems~~.~~ and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated ~~Interactive Remote Access, and (ii) system-to-system~~ remote access ~~with a vendor(s).~~.

M1. Evidence shall include~~-~~ one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- ~~Link to the~~ Implementation Plan ~~and other important associated documents.~~ for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	

~~Rationale~~

~~Requirement R1:~~

~~The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):~~

~~(1) Software integrity and authenticity;~~
~~(2) Vendor remote access;~~
~~(3) Information system planning; and~~
~~(4) Vendor risk management and procurement controls.~~

~~The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.~~

~~Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).~~

~~Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.~~

~~Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.~~

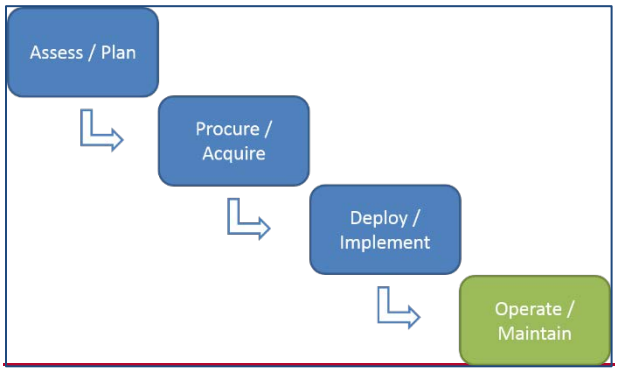
~~The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the~~

~~awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.~~

~~Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.~~

~~Notional BES Cyber System Life Cycle~~



~~Requirement R2:~~

~~The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).~~

~~Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:~~

- ~~NERC or the E-ISAC~~
- ~~ICS-CERT~~
- ~~Canadian Cyber Incident Response Centre (CCIRC)~~

~~Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).~~2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-2

Proposed Reliability Standard CIP-005-7
Clean

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised

7	11/05/2020	Adopted by the NERC Board of Trustees.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-2

Proposed Reliability Standard CIP-005-7
Redline to Last Approved (CIP-005-6)

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~6~~7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

~~All BES Facilities.~~

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~6~~7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" ~~-~~The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). ~~-~~Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. ~~-~~Examples in the standards include the personnel risk assessment program and the personnel training program. ~~-~~The full implementation of the CIP Cyber Security Standards could also be referred to as a program. ~~-~~However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-~~6~~7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~6~~7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. -Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised

7	11/05/2020	Adopted by the NERC Board of Trustees.	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

~~However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.~~

~~For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.~~

~~If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.~~

~~The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.~~

~~This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run~~

~~between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.~~

~~As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.~~

~~The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.~~

~~**Requirement R2:**~~
~~See Secure Remote Access Reference Document (see remote access alert).~~

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

~~Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.~~

~~Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.~~

~~The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).~~

~~The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators~~

~~**Summary of Changes:** This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.~~

~~**Reference to prior version:** (Part 2.1) New~~

~~**Change Rationale:** (Part 2.1)~~
~~*This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*~~

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-3

Proposed Reliability Standard CIP-010-4
Clean

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS;	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to:

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA		• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated:	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA	required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity failed to document or implement one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-4,	Removable Media, but failed to implement the Removable Media sections according to CIP-010-4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-4, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R4, Attachment 1, Section 1.2. (R4)	Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1
Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-3

Proposed Reliability Standard CIP-010-4
Redline to Last Approved (CIP-010-3)

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-~~3~~4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

~~All BES Facilities.~~

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~3~~4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be

referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves.~~-~~ Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. ~~-~~The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002~~-5.1~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced

high impact BES Cyber System or medium impact BES Cyber System. -Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS;	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to:

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA		• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated:	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA	required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including ~~of~~ the date of the test.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity documented its plan(s) for Transient Cyber Assets and	The Responsible Entity failed to document or implement one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~3~~4,	Removable Media, but failed to implement the Removable Media sections according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for	plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-~~3~~4, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R4, Attachment 1, Section 1.2. (R4)	Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~3~~4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-~~3~~4 - Attachment 1
Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-~~3~~4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Baseline Configuration~~

~~The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.~~

~~Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or~~

~~other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.~~

~~Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:~~

~~Asset #051028 at Substation Alpha~~

- ~~R1.1.1 – Firmware: [MANUFACTURER] [MODEL] XYZ-1234567890-ABC~~
- ~~R1.1.2 – Not Applicable~~
- ~~R1.1.3 – Not Applicable~~
- ~~R1.1.4 – Not Applicable~~
- ~~R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823~~

~~Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.~~

~~Cyber Security Controls~~

~~The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.~~

~~Test Environment~~

~~The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.~~

~~Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).~~

~~Software Verification~~

~~The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.~~

~~NIST SP 800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP 800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.~~

~~In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:~~

- ~~Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.~~
- ~~Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.~~
- ~~Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.~~
- ~~Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.~~
- ~~Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.~~

~~Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:~~

- ~~Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.~~
- ~~Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.~~
- ~~Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.~~
- ~~Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)~~

~~**Requirement R2:**~~

~~The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.~~

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

~~connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.~~

~~Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:~~

- ~~1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.~~
- ~~1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.~~
- ~~1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,~~

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

~~Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

- ~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~
- ~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.~~
- ~~Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.~~
- ~~When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.~~

~~Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.~~

- ~~For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.~~
- ~~Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that~~

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low-tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

~~Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.~~

- ~~Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.~~
- ~~Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.~~
- ~~Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.~~
- ~~When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.~~

~~Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

- ~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~
- ~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~
- ~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~
- ~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~
- ~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.~~

~~Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.~~

~~Requirement R4, Attachment 1, Section 3 - Removable Media~~

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.~~

- ~~Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.~~
- ~~Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.~~

~~Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.~~

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the

~~SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6[1]. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber

[1] In the event CIP-002-6 has not yet been approved or otherwise made effective in the applicable jurisdiction, please refer to the Implementation Plan associated with CIP-002-5.1a.

System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standards meet or exceed the criteria.

1. **Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]**

The proposed Reliability Standards enhance the cybersecurity posture of the electric industry by broadening the applicable systems to which the protections in the Supply Chain Standards apply. Consistent with the directive in Order No. 850, the supply chain requirements in CIP-013-2, CIP-005-7, and CIP-010-4 apply to Electronic Access Control or Monitoring Systems ("EACMS"). Moreover, consistent with the recommendations in the NERC Supply Chain Report, the supply chain requirements also apply to Physical Access Control Systems ("PACS"). As such, the proposed Reliability Standards enhance the reliability of the BES by addressing supply chain risk management for EACMS and PACS.

2. **Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]**

The proposed Reliability Standards are clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standards

---

1 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Order No. 672, 114 FERC ¶ 61,104, *order on reh'g,* Order No. 672-A, 114 FERC ¶ 61,328 (2006) [hereinafter Order No. 672].

2 *See* Order No. 672, *supra* note 1, at P 324.

3 *See* Order No. 672, *supra* note 1, at PP 322, 325.

apply to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standards clearly articulate the actions that such entities must take to comply with the standard.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment, as discussed further in Exhibit D. The assignment of the severity level for each VSL is consistent with the corresponding requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standards include clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner. [5]

The proposed Reliability Standards contain measures that support the requirements by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirements will be enforced and help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party. The measures are substantively unchanged from the currently effective version of the standard.

---

4 *See* Order No. 672, *supra* note 1, at P 326.

5 *See* Order No. 672, *supra* note 1, at P 327.

5. **Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]**

The proposed Reliability Standards achieve the reliability goals effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standards clearly articulate the security objective that applicable entities must meet and provide entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

6. **Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]**

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. The proposed Reliability Standards broaden the applicable systems to which the Supply Chain Standards apply. Furthermore, the proposed Reliability Standards go beyond the Order No. 850 directive with minimal to no use of subsets of EACMS and PACS.

7. **Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]**

The proposed Reliability Standards apply throughout North America and do not favor one geographic area or regional model.

---

6 *See* Order No. 672, *supra* note 1, at P 328.

7 *See* Order No. 672, *supra* note 1, at PP 329-30.

8 *See* Order No. 672, *supra* note 1, at P 331.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standards have no undue negative impact on competition. The proposed Reliability Standards require the same performance by each of the applicable Functional Entities. The proposed Reliability Standards do not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed implementation period for the proposed Reliability Standards is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must apply appropriate protections on EACMS and PACS.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standards were developed in accordance with NERC's Commission-approved, ANSI-accredited processes for developing and approving Reliability Standards. Exhibit E includes a summary of the development proceedings and details the processes followed to develop the proposed Reliability Standards. These processes included, among other things, comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum, and the last additional ballot and final ballot exceeded the required ballot pool approval levels.

---

9 *See* Order No. 672, *supra* note 1, at P 332.

10 *See* Order No. 672, *supra* note 1, at P 333.

11 *See* Order No. 672, *supra* note 1, at P 334.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standards. No comments were received that indicated the proposed Reliability Standards conflict with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standards are just and reasonable were identified.

---

12 *See* Order No. 672, *supra* note 1, at P 335.

13 *See* Order No. 672, *supra* note 1, at P 323.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D

Consideration of Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system for supply chain requirements. Proposed CIP-005-7 Requirement R3 is a new requirement that includes methods to determine and terminate authenticated vendor-initiated remote connections for EACMS, which is similar to requirements in Parts 2.4 and 2.5 for other applicable systems. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system for supply chain requirements. Proposed CIP-005-7 Requirement R3 is a new requirement that requires processes that include methods to determine and terminate authenticated vendor-initiated remote connections for PACS, which is similar to requirements in Parts 2.4 and 2.5 for other applicable systems.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-1

Technical Rationale CIP-013-2

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

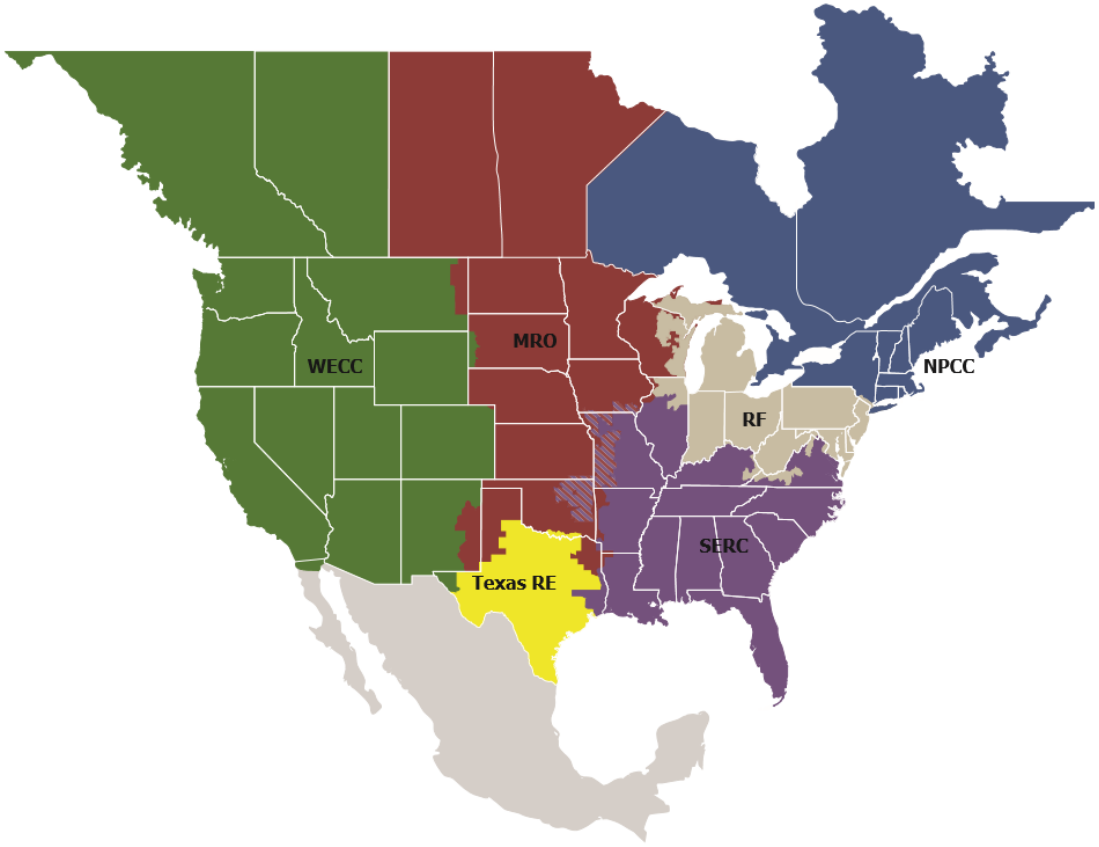
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

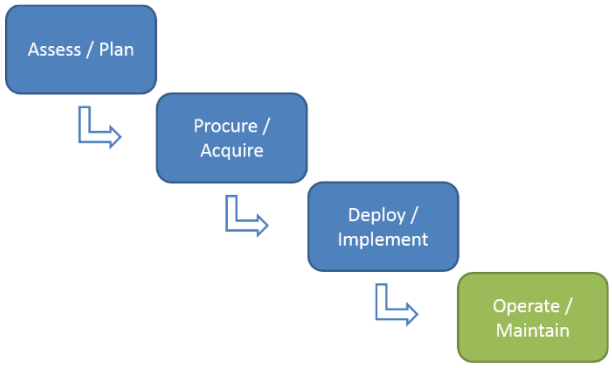
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

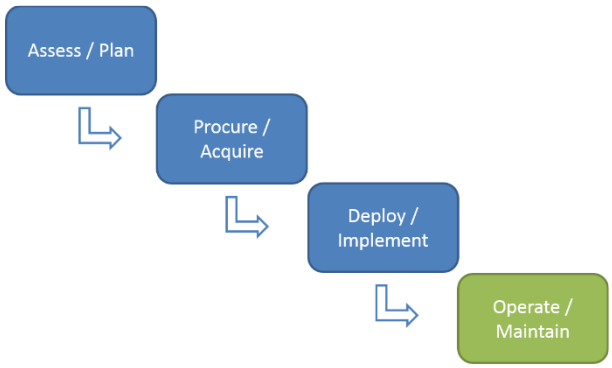
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-2

Technical Rationale CIP-005-7

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

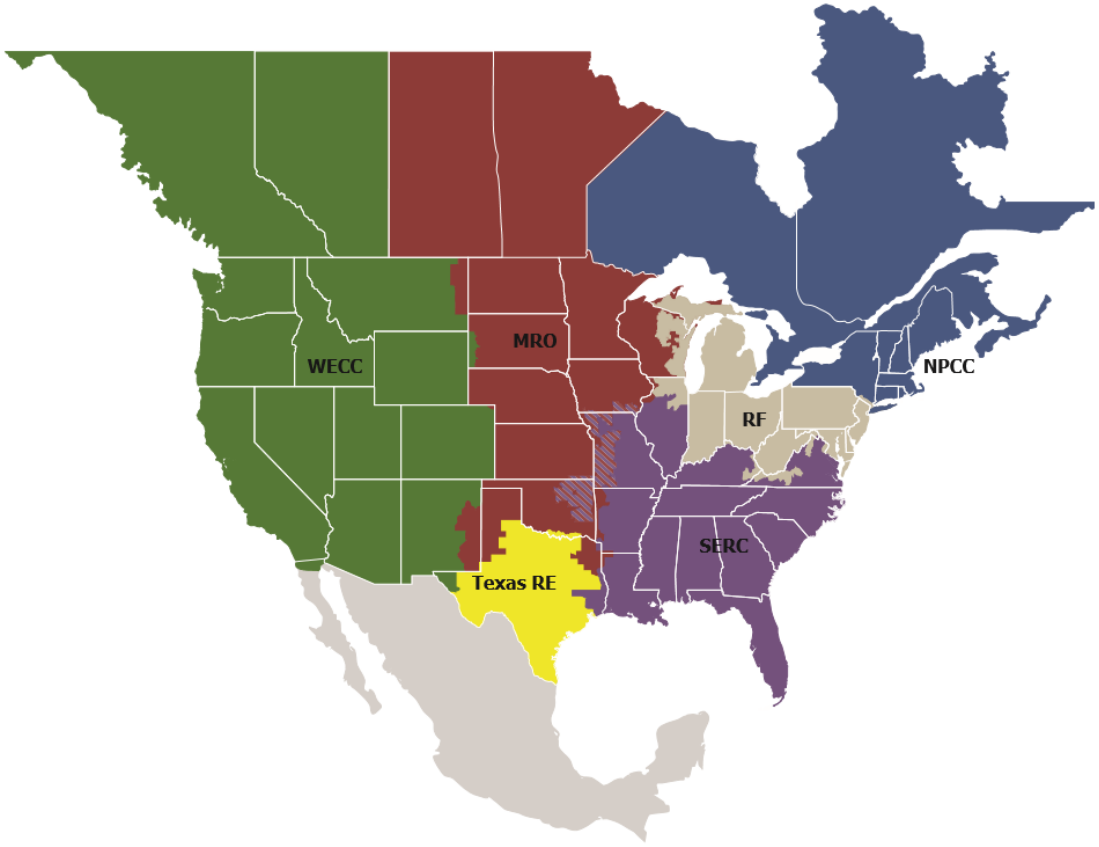
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-3

Technical Rationale CIP-010-4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

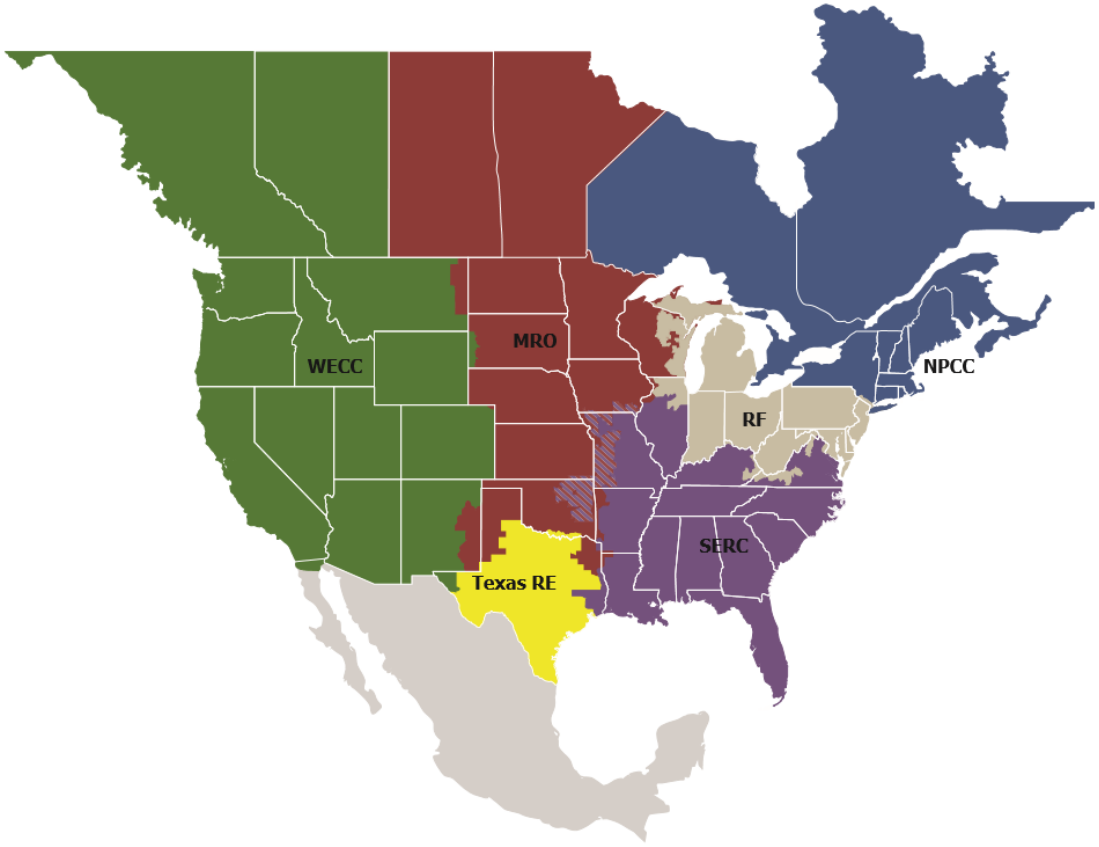
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F

Implementation Guidance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F-1

Implementation Guidance CIP-013-2

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for Reliability Standard CIP-013-2

October 2020

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

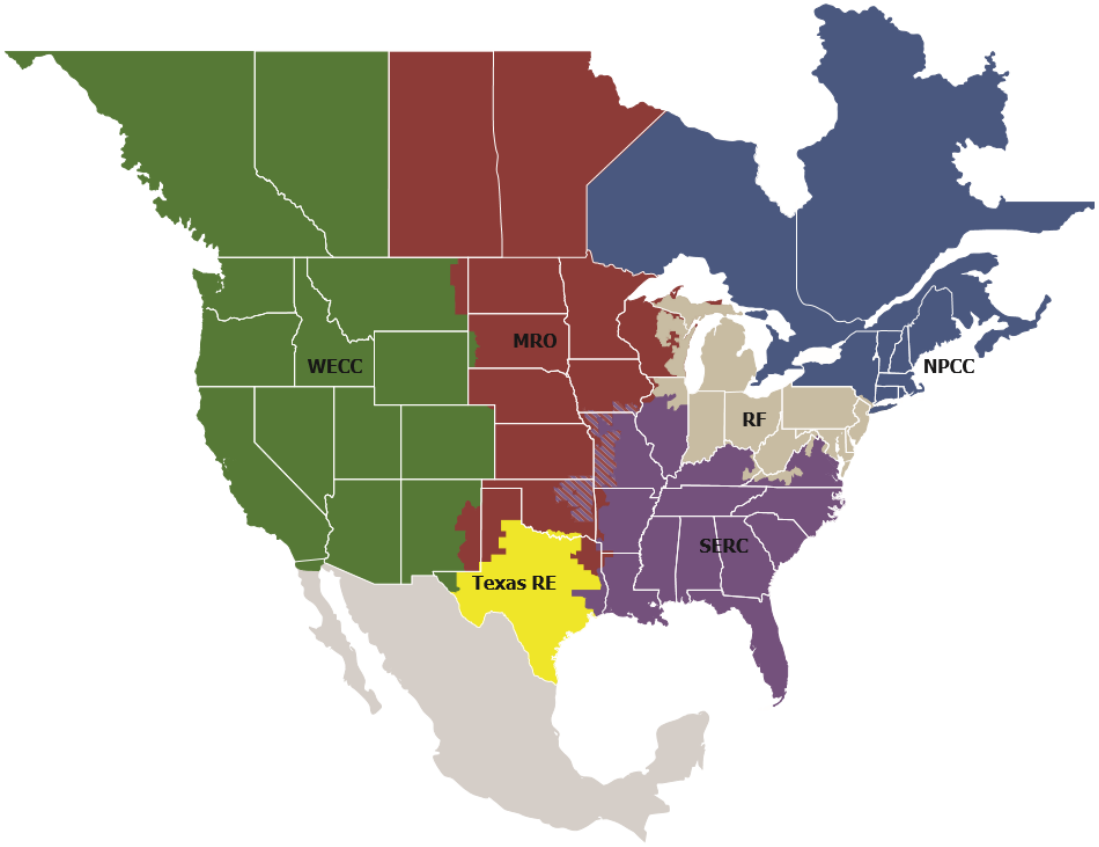
Table of Contents

Preface

*Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. T*he vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1] and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

1.2.6. *Coordination of controls for vendor-initiated remote access.*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-2.

> *Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.*

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

  1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review)

approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:
    - Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
    - Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2.

Requirement R3

R3. *Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F-2

Implementation Guidance CIP-005-7

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

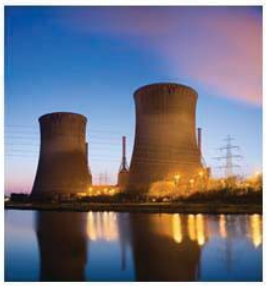
DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

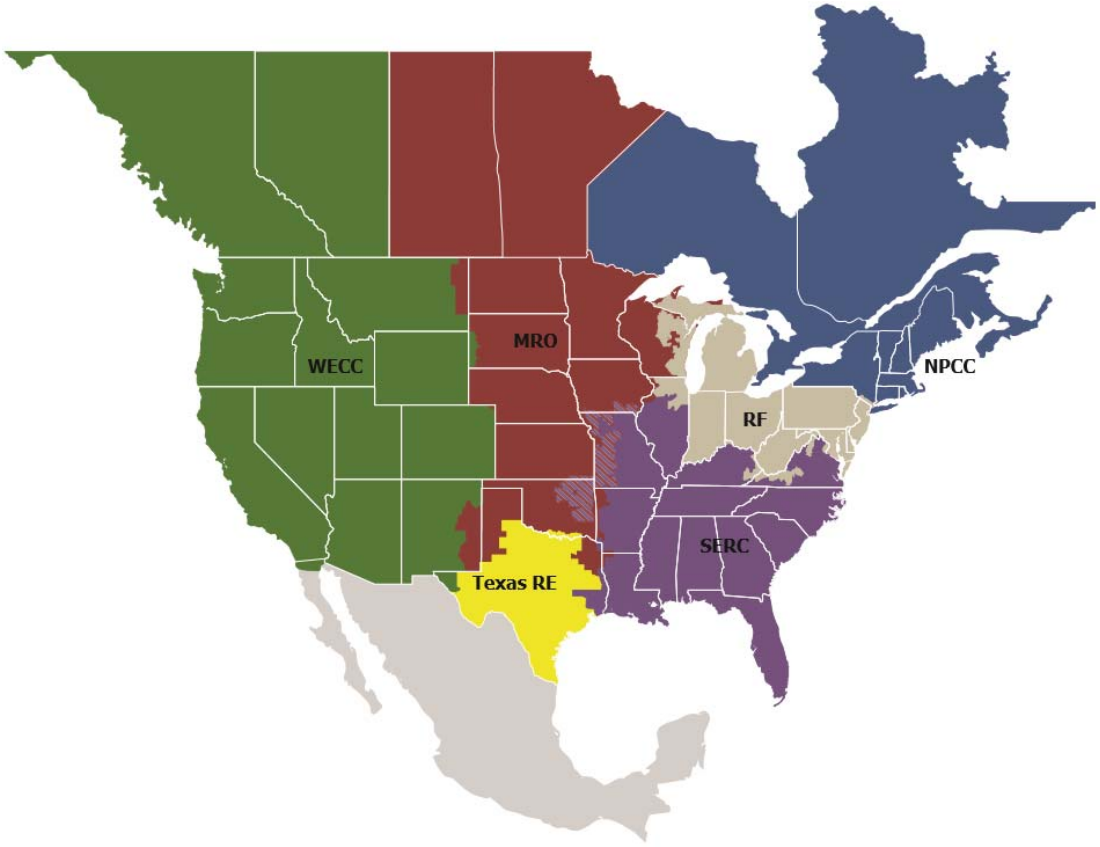
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements Parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method to determine authenticated vendor-initiated remote connections is documented and the ability to disable that remote connection is required. For example, if an entity utilizes its corporate remote access solution to allow remote connection into its PACS, the entity would need to document the authenticated remote connection method and develop a process to terminate such connections after authentication. Some examples of how an entity might terminate these connections may be as simple as, but are not limited to actions like disabling a token or certificate for a vendor account(s), suspending or deleting the vendor account(s) in Active Directory, blocking the vendor's IP range, or physically disconnecting a network cable.

Intermediate Systems (a subset of EACMS) use is not a requirement for remote access to other EACMS, lessening the potential of the recursive requirement ("hall of mirrors") However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS (within the Electronic Security Perimeter), the process of terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor attempts the remote access connection, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable the vendor's ability to make a connection. The remote access vendor will attempt to "connect" with the EACMS however, after unsuccessful authentication the connection attempt will be terminated. This scenario illustrates a method to disallow vendor-initiated remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and network topologies to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes

to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F-3

Implementation Guidance CIP-010-4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

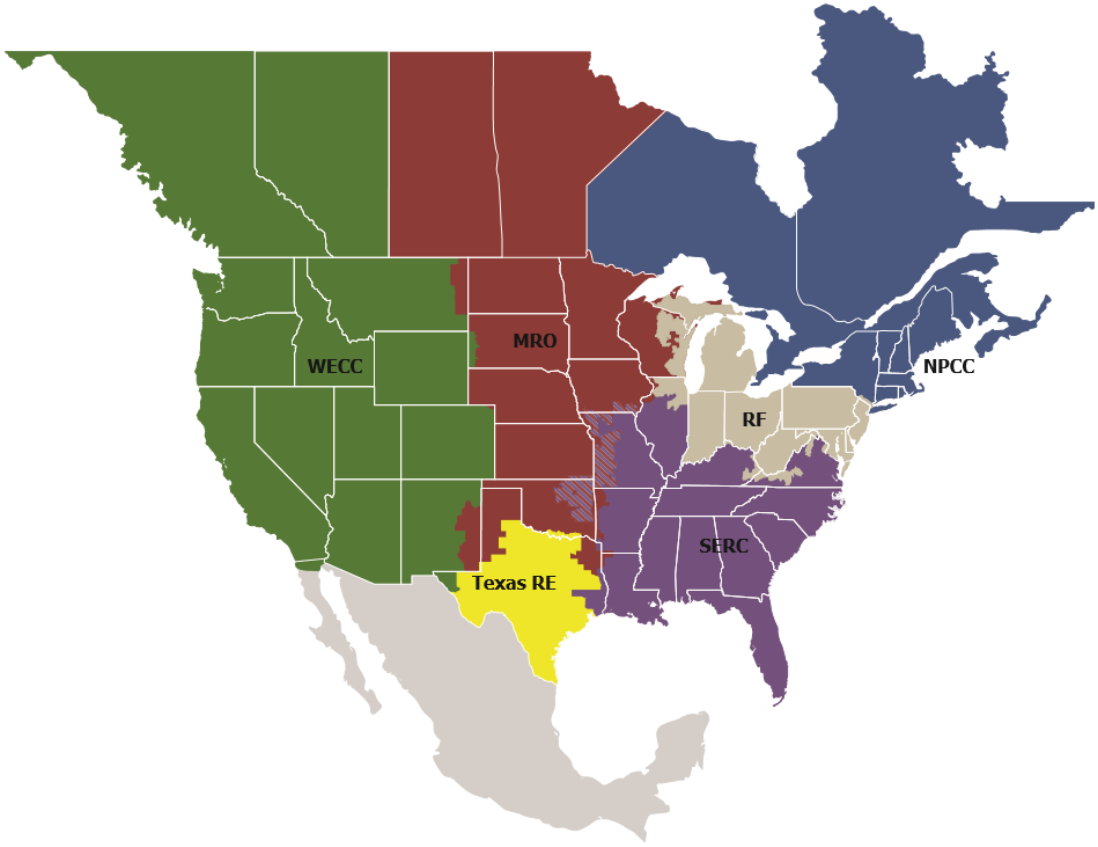
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirements R1 and R2

The VRFs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirements R1 and R2

The VSLs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2

The VRFs for all requirements in CIP-013-2 did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirements R1 and R2

The VSLs did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirements.

VSL Justification for CIP-013-2, Requirement R3

The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to authenticate vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate established vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method for detecting vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
		method to terminate authenticated vendor-initiated remote connections for EACMS (3.2).	

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium for Requirement R3, which addresses Vendor Remote Access Management for EACMS and PACS, is consistent with Reliability Standard CIP-005-7 Requirement R2, which addresses Remote Access Management and includes requirements for vendor access management for high and certain medium impact BES Cyber Systems and associated PCA.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser-risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit H

Summary of Development History and Complete Record of Development

Summary of Development History

The following is a summary of the development record for proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team ("SDT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the SDT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2019-03 Cyber Security Supply Chain Risks SDT members is included in **Exhibit I**.

II. Standard Development History

A. Standard Authorization Request Development

On June 26, 2019, the Standards Committee authorized posting a Standards Authorization Request ("SAR") to address Commission directives from Order No. 850[3] and NERC staff recommendation from the Supply Chain Report[4] for a 30-day informal comment period from July 2, 2019 through August 1, 2019 and authorized the solicitation of SDT members.[5] Based on

[1] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2018).

[2] The NERC *Standard Processes Manual* is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

[3] *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018).

[4] NERC, *NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, Docket No. RM17-13-000 (2019), https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Supply%20Chain%20Report%20Filing.pdf

[5] NERC, *Meeting Minutes – Standards Committee Meeting* (June 26, 2019), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20June%20Meeting%20Minutes_Approved_072419.pdf.

comments received, the SDT revised the SAR. The Standards Committee accepted the revised SAR on October 23, 2019.[6]

B. First Posting - Comment Period, Initial Ballot, and Non-binding Poll

On January 22, 2020, the Standards Committee authorized initial posting of proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4, the associated Implementation Plan and other associated documents for a 45-day formal comment period from January 27, 2020 through March 11, 2020, with a parallel initial ballot and non-binding poll on the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") held during the last 10 days of the comment period from March 2, 2020 through March 11, 2020.[7] The initial ballot for proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 received 50.51 percent approval, reaching quorum at 88.67 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 47.12 percent supportive opinions, reaching quorum at 86.62 percent of the ballot pool. There were 66 sets of responses, including comments from approximately 137 different individuals and approximately 96 companies, representing all 10 industry segments.[8]

C. Second Posting - Comment Period, Additional Ballot, and Non-binding Poll

Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4, the associated Implementation Plan and other associated documents were posted for a 45-day formal comment period from May 7, 2020 through June 22, 2020, with a parallel additional ballot and non-binding

---

[6] NERC, *Meeting Minutes – Standards Committee Meeting* (Oct. 23, 2019), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20October%20Meeting%20Minutes_Approved%20112019.pdf.

[7] NERC, *Standards Committee Agenda Package*, Agenda Item 5 (Project 2019-03 Cyber Security Supply Chain Risks (CIP-013-2, CIP005-7, CIP-010-4)) *available at* https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_January_22_2020.pdf.

[8] NERC, *Consideration of Comments – CIP-013-2, CIP-005-7, CIP-010-4*, Project 2019-03 Cyber Security Supply Chain Risks (May 2020), https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Supply_Chain_Consideration_of_Comments_05072020.pdf.

poll held during the last 10 days of the comment period from June 12, 2020 through June 22, 2020. The additional ballot for proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 received 34.44 percent approval, reaching quorum at 79 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 33.14 percent supportive opinions, reaching quorum at 76.41 percent of the ballot pool. There were 75 sets of responses, including comments from approximately 183 different individuals and approximately 124 companies, representing all 10 industry segments.[9]

D. Third Posting - Comment Period, Initial Ballot, and Non-binding Poll

Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4, the associated Implementation Plan and other associated documents were posted for a 45-day formal comment period from July 28, 2020 through September 10, 2020, with a parallel additional ballot and non-binding poll held during the last 10 days of the comment period from September 1, 2020 through September 10, 2020. The additional ballot for proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 received 80.78 percent approval, reaching quorum at 79.41 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 76.97 percent supportive opinions, reaching quorum at 76.9 percent of the ballot pool. There were 59 sets of responses, including comments from approximately 135 different individuals and approximately 85 companies, representing all 10 industry segments.[10]

[9] NERC, *Consideration of Comments – CIP-013-2, CIP-005-7, CIP-010-4*, Project 2019-03 Cyber Security Supply Chain Risks (July 2020), https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Supply_Chain_Response_to_Comments_08072020.pdf.

[10] NERC, *Consideration of Comments – CIP-013-2, CIP-005-7, CIP-010-4*, Project 2019-03 Cyber Security Supply Chain Risks (Oct. 7, 2020), https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Supply_Chain_Consideration_of_Comments_10072020.pdf.

E. Final Ballot

Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 were posted for a 10-day final ballot period from October 7, 2020 through October 16, 2020. The ballot for proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 and associated documents reached quorum at 83.56 percent of the ballot pool, receiving affirmative support from 76.76 percent of the voters.

F. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 on November 5, 2020.[11]

[11] NERC, *Board of Trustees Agenda Package*, Agenda Item 5.a. (Project 2019-03 Cyber Security Supply Chain Risks (CIP-013-2, CIP005-7, CIP-010-4)) *available at* https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_of_Trustees_November-5_2020_Agenda_Package_Attendees_ONLY.pdf.

Complete Record of Development

Project 2019-03 Cyber Security Supply Chain Risks

Related Files

Status

The 10-day final ballot concluded **8 p.m. Eastern, Friday, October 16, 2020** for the following:

*CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)

*CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments

*CIP-013-2 – Cyber Security - Supply Chain Risk Management

*Implementation Plan

The voting results can be accessed via the link below. The standards will be submitted to the Board of Trustees for adoption then filed with the appropriate regulatory authorities.

Background
This project will address the directives issued by FERC in Order No. 850 to modify the Supply Chain Standards. FERC directed NERC to submit modifications to address EACMSs, specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850. In addition, NERC also recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. The modifications to address PACS do not have a regulatory deadline, but will be addressed by this project.

Standard(s) Affected – CIP-005-6 - Cyber Security - Electronic Security Perimeter(s) | CIP-010-3 - Cyber Security - Configuration Change Management and Vulnerability Assessments | CIP-013-1 - Cyber Security - Supply Chain Risk Management.

Purpose/Industry Need
This project will address the directives issued by FERC in Order No. 850. This project will also address NERC staff recommendation from the Supply Chain Report.

Subscribe to this project's observer distribution list
Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-005-7 **(88)** Clean | **(89)** Redline to Last Posted | **(90)** Redline to Last Approved CIP-010-4 **(91)** Clean | **(92)** Redline to Last Posted | **(93)** Redline to Last Approved CIP-013-2 **(94)** Clean | **(95)** Redline to Last Posted | **(96)** Redline to Last Approved Implementation Plan **(97)** Clean | **(98)** Redline **Supporting Materials** **(99)** VRF/VSL Justifications Consideration of Issues and Directives **(100)** Clean | **(101)** Redline to Last Posted Summary of Changes **(102)** CIP-005-7 **(103)** CIP-010-4 **(104)** CIP-013-2	Final Ballot **(112)** Info Vote	10/07/20 - 10/16/20	**(113)** Ballot Results	

Technical Rationale **(105)** CIP-005-7 **(106)** CIP-010-4 (**107)** CIP-013-2 Implementation Guidance CIP-005-7 **(108)** Clean | **(109)** Redline to Last Posted **(110)** CIP-010-4 **(111)** CIP-013-2				
Draft 3 CIP-005-7 **(52)** Clean | **(53)** Redline to Last Posted | **(54)** Redline to Last Approved CIP-010-4 **(55)** Clean | **(56)** Redline to Last Posted CIP-013-2 **(57)** Clean | **(58)** Redline to Last Posted Implementation Plan **(59)** Clean | **(60)** Redline to Last Posted **Supporting Materials** **(61)** Unofficial Comment Form (Word) VRF/VSL Justifications **(62)** Clean | **(63)** Redline to Last Posted Consideration of Issues and Directives **(64)** Clean | **(65)** Redline to Last Posted **(66)** CIP-005-7 Summary of Changes **(67)** CIP-010-4 Summary of Changes **(68)** CIP-013-2 Summary of Changes Technical Rationale CIP-005-7 **(69)** Clean | **(70)** Redline to Last Posted CIP-010-4 **(71)** Clean | **(72)** Redline to Last Posted CIP-013-2 **(73)** Clean | **(74)** Redline to Last Posted Implementation Guidance CIP-005-7 **(75)** Clean | **(76)** Redline to Last Posted	Additional Ballot and Non-binding Poll **(84)** Updated Info **(85)** Info Vote	09/01/20 - 09/10/20	**(86)** Ballot Results **(87)** Non-binding Poll Results	
	Comment Period **(81)** Info Submit Comments	07/28/20 - 09/10/20	**(82)** Comments Received	**(83)** Consideration of Comments

CIP-010-4 **(77)** Clean | **(78)** Redline to Last Posted CIP-013-2 **(79)** Clean | **(80)** Redline to Last Posted				
Draft 2 CIP-005-7 **(26)** Clean | **(27)** Redline to Last Posted CIP-010-4 **(28)** Clean | **(29)** Redline to Last Posted CIP-013-2 **(30)** Clean | **(31)** Redline to Last Posted Implementation Plan **(32)** Clean | **(33)** Redline to Last Posted **Supporting Materials** **(34)** Unofficial Comment Form (Word) **(35)** VRF/VSL Justifications Consideration of Issues and Directives **(36)** Clean | **(37)** Redline to Last Posted **(38)** CIP-005-7 Summary of Changes Technical Rationale **(39)** CIP-005-7 **(40)** CIP-010-4 **(41)** CIP-013-2 Implementation Guidance **(42)** CIP-005-7 **(43)** CIP-010-4 **(44)** CIP-013-2	Additional Ballot and Non-binding Poll **(48)** Updated Info **(49)** Info Vote	06/12/20 - 06/22/20	**(50)** Ballot Results **(51)** Non-binding Poll Results	
	Comment Period **(45)** Info Submit Comments	05/07/20 - 06/22/20	**(46)** Comments Received	**(47)** Consideration of Comments
Draft 1 CIP-005-7 **(9)** Clean | **(10)** Redline CIP-010-4 **(11)** Clean | **(12)** Redline CIP-013-2 **(13)** Clean | **(14)** Redline **(15)** Implementation Plan **Supporting Materials** **(16)** Unofficial Comment Form (Word) **(17)** VRF/VSL Justifications	Initial Ballot **(22)** Updated Info **(23)** Info Vote	03/02/20 - 03/11/20	**(24)** Ballot Results **(25)** Non-binding Poll Results	
	Comment Period **(19)** Info Submit Comments	01/27/20 - 03/11/20	**(20)** Comments Received	**(21)** Consideration of Comments
	Join Ballot Pools	01/27/20 - 02/25/20		

(18) Consideration of Issues and Directives				
Standard Authorization Request (SAR) **(7)** Clean | **(8)** Redline	The Standards Committee accepted the SAR on October 23, 2019			
Drafting Team Nominations **Supporting Materials** **(5)** Unofficial Nomination Form (Word)	Nomination Period **(6)** Info Submit Nominations	07/02/19 - 08/01/19		
(1) Standard Authorization Request **Supporting Materials** **(2)** Unofficial Comment Form (Word)	Comment Period **(3)** Info Submit Comments	07/02/19 - 08/01/19	**(4)** Comments Received	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to Cyber Security – Supply Chain Controls Standard		
Date Submitted:	June 26, 2019		
SAR Requester			
Name:	Soo Jin, Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☒ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 directing NERC to develop modifications to the Supply Chain Standards. In addition, NERC published a Cyber Security Supply Chain Risks report and recommendations for additional modifications to the Supply Chain Standards.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the directives issued by FERC in Order No. 850 to modify the Supply Chain Standards. FERC directed NERC to submit modifications to address EACMSs, specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850. In addition, NERC also recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. The modifications to address PACS do not have a regulatory deadline, but will be addressed by this project.			

Requested information
Project Scope (Define the parameters of the proposed project):
This project will address the directives issued by FERC in Order No. 850. This project will also address NERC staff recommendation from the Supply Chain Report to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
Consider recommendations to revise the Supply Chain Reliability Standards to include: (i) EACMSs, specifically those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems; and (ii) PACSs that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time. However, a question will be asked during the SAR comment period to ensure all aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP Standard
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-03 Cyber Security Supply Chain Risks

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-03 Cyber Security Supply Chain Risks Standard Authorization Request (SAR).** Comments must be submitted by **8 p.m. Eastern, Thursday, August 1, 2019.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 directing NERC to develop modifications to the Supply Chain Standards. FERC directed NERC to submit modifications to address EACMSs, specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850. In addition, NERC also recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. The modifications to address PACS do not have a regulatory deadline, but will be addressed by this project.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

2. Provide any additional comments for the SAR drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Informal Comment Period Open through August 1, 2019

Now Available

A 30-day informal comment period for the **Project 2019-03 Cyber Security Supply Chain Risks Standard Authorization Request (SAR)**, is open through **8 p.m. Eastern, Thursday, August 1, 2019**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Linda Jenkins. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The SAR drafting team will review all responses received during the comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	Project 2019-03 Cyber Security Supply Chain Risks
Comment Period Start Date:	7/2/2019
Comment Period End Date:	8/1/2019
Associated Ballots:	

There were 29 sets of responses, including comments from approximately 80 different people from approximately 61 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
Duke Energy		1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC

	Katherine Street				Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Adrianne Collins	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Jones	National Grid	3	NPCC

Sean Cavote	PSEG	4	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Mike Forte	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC

					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

Comments: GTC encourages limiting the scope of the SAR to address the directive issued by FERC in order 850 due to the following basis:

· Entities have not yet fully implemented the CIP-013 programs which apply to high and medium impact BES Cyber Systems; and therefore such addition at this immature stage in the implementation cycle could over complicate and disrupt the focused attention necessary to fully implement in its current state.

· The additional undirected scope could cause opposition by industry and thus delays in NERC meeting FERC's Standard revision submittal deadline "24 months from the effective date of Order No. 850".

· The current version of CIP-013-1 already requires entities to identify and assess risks of vendor services for installing BES Cyber Assets (equipment/software). Such service type vendors that can perform installation services at high or medium impact locations are required to have "CIP" physical access via each entities CIP program. Vendors that do not have physical access (escorted visitor access) can also be identified and assessed accordingly by each entity. Therefore, the physical access component will be assessed and addressed by each entity as part of implementation of CIP-013-1 R1.1 already.

· PACs components installed at physical security perimeters housing BES Cyber Systems are video monitored/protected under the CIP program. Any compromise at the device level performed in the cyber realm must ultimately be accompanied by physical presence in order to gain access inside the physical security perimeter. Unauthorized physical access would be recognized and acted upon in very short fashion even if material was compromised at the manufacturer supplier "supply chain" level. Therefore, GTC sees the addition of PACS in CIP-013-2 as premature at this time and adequately monitored (and risk managed) by CIP programs.

For the various reasons above, GTC encourages NERC to be patient and let entities implement CIP-013 programs which will apply to high/medium impact BES Cyber Systems and EACMS before attempting to expand the scope at such an early stage in the implementation and audit cycle.

Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	

GSOC encourages limiting the scope of the SAR to address the directive issued by FERC in order 850 due to the following basis:

- Entities have not yet fully implemented the CIP-013 programs which apply to high and medium impact BES Cyber Systems; and therefore such addition at this stage in the implementation cycle could over complicate and disrupt the focused attention necessary to fully implement in its current state.
- The additional undirected scope could cause opposition by industry and thus delay NERC meeting FERC's Standard revision submittal deadline "24 months from the effective date of Order No. 850".

For the various reasons above, GSOC encourages NERC to be patient and let entities implement CIP-013 programs which will apply to high/medium impact BES Cyber Systems and EACMS before attempting to expand the scope at such an early stage in the implementation and audit cycle.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP agrees with the proposed scope as described in the SAR primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES. These systems have also been found to be a gateway to other systems. Even if only the EACMS and PACs systems were compromised it could result in unauthorized physical and logical access to protected systems.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company supports including EAMCS of the proposed Supply Chain Standard that apply to access control and exclude monitoring and logging functions. Southern also supports possibly changing the complete definition of EACMS that would apply to the this standard and other CIP Standards and recommends the SDT to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. Southern does however disagree with NERC including PACS assets into the scope of CIP-013 Supply Chain Standard. There is not a clear path to define who could or would be the potential vendor of PACS assets; the third party reseller or the manufacturer. The company who ultimately supplies Southern with the assets may not be the party who purchases the assets on behalf of Southern as in the case with controller panels. PACS workstations which could be Dell machines would not be purchased directly from Dell but from a reseller who provides for all of Southern, but not necessarily for PACS specifically. The risk based approach for PACS assets would be very limited in scope.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO appreciates the efforts of CIPC Supply Chain Working Group (SCWG) in drafting these guidelines. IESO supports the comments submitted by NPCC.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	

FERC Order No. 850 directed modifications to the supply chain risk management Reliability Standards to include EACMS. Paragraph 6 stated that more study is necessary to determine the impact of PACS and PCAs.

NERC published its study and recommendations in the May 17, 2019, Cyber Security Supply Chain Risks Staff Report and Recommended Actions. That report recommends addressing PACS in the Cyber Security Supply Chain standards, but not including PCAs at this time.

The scope of this SAR is consistent with the FERC order and the findings of the NERC study.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

Although addressing PACS is not a directive from FERC, it seems prudent to expand the scope of the SAR beyond the FERC order to include PACS, since the standard is being modified.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

- PAC agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) specifically involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities
- PAC agrees with including Physical Access Control Systems (PACS) that provide physical access control, excluding alarming and logging, to high and medium impact BES Cyber Systems, primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES

Likes 0	
Dislikes 0	

Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
NERC is recommending addressing PACS as part of this SAR. NERC needs to consider the challenges related to supply chain for end-point PACS such as control panels in fire control rooms, communication facilities, etc... Many transmission and generation entities rely on large and small contract companies to maintain these end-point control panel PACS, and attempting to identify chipset software and/or operating system suppliers or manufacturers will be challenging and in some cases not feasible. In addition, depending on an entities physical and electronic protections of PACS, the risk of Supply Chain outweighs the benefit. NERC may desire to consider compensating controls options within Supply Chain for PACS which can be verified by the contract or vendor support companies.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	

Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NVE agrees with the SAR on inclusion of EACMS and PACS that are associated with High and Medium Impact BCS.	
Likes 0	
Dislikes 0	
Response	
Nick Batty - Keys Energy Services - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Zwergel - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katherine Street - Duke Energy - 1,3,5,6 - SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
NVE provides the following recommendations for the SDT: • Language needs to be consistent and take the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs • When revising CIP-013-1, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from the PACS definition per the NERC Glossary.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
GSOC recommends adding a review of the definition(s) of EACMS, PACS, and to define new term(s) accordingly to exclude monitoring and logging from the addition of EACMSs and/or to exclude alarming/alerting and logging from the PACs definition as part of the scope of this SAR.	

Specifically, this project could consider separate definitions to clarify and distinguish access/control type systems such as Electronic Access Control Systems (EACS) and PACS, from alarming/logging type systems such as Electronic Alarming, Monitoring or Logging Systems (EAMLS) as separate NERC defined terms. This clarity would appropriately categorize new alarming/alerting/logging “only” type systems as BESCI repositories as well as distinguish access/control type systems in an unbundled manner.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

GTC recommends to add a review of the definition(s) of EACMS, PACS, and to define new term(s) accordingly to exclude monitoring and logging from the addition of EACMSs and/or to exclude alarming/alerting and logging from the PACs definition as part of the scope of this SAR.

Specifically, this project could consider separate definitions to clarify and distinguish access/control type systems such as Electronic Access Control Systems (EACS) and PACS, from alarming/logging type systems such as Electronic Alarming, Monitoring or Logging Systems (EAMLS) as separate NERC defined terms. This clarity would appropriately categorize new alarming/alerting/logging “only” type systems as BESCI repositories.

Likes 0	
Dislikes 0	

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	
Comment	

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Yes

No

Comments:

- PAC agrees with the Standard Authorization Request (SAR) modifications to include Electronic Access Control or Monitoring Systems (EACMS) specifically involved with medium and high impact BES Cyber Systems (BCS), excluding those devices which handle only monitoring and/or logging capabilities
- PAC agrees with including Physical Access Control Systems (PACS) that provide physical access control, excluding alarming and logging, to high and medium impact BES Cyber Systems, primarily because the exclusion of the EACMS and PACs could result in unauthorized access to the BES

1. Provide any additional comments for the SAR drafting team to consider, if desired.

Comments:

- “R1.1 should be read as “The plan(s) shall include one or more process(es) for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services …” followed by the rest of R1.1.”
- There is a missing component: Mitigate:
    - This is the second word in the “Purpose” of the Standard, but it is not listed anywhere else in the entire Standard – basically this leaves an action intended, but not stated to perform
- If low impact BCS are included in the scope of CIP-013, PAC recommends the standard allow entities to make a risk-based decision to purchase and implement a product in the absence of that product’s vendor being able to meet the entity’s requirements (e.g., R1.2.1 through R1.2.6)
- Will CIP Exceptional Circumstances be considered for Cyber Assets and software procured for emergencies?

- Language needs to be consistent and take the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs
- When revising CIP-013-1, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from the PACS definition per the NERC Glossary

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

Thank you for the opportunity to comment

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	
Document Name	

Comment

When revising the supply chain risk management Reliability Standards, keep in mind the exclusion of “locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers” from PACSs per the NERC Glossary definition.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment
Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment
The Project 2016-02 SDT is strongly considering changes to the definition aand classification of EACMS to more fully address the realities and technical concerns of “access control” vs “access monitoring” systems and the need to consider 3rd party services for best practices in enterprise monitoring. In light of the proposed separation of EACMS into EAMS and EACS, the directive to modify within 24 months of Order 850 could have significant impact on any effort to evaluate the supply chain for products and services that the RE does not have on-premises or that may be under contractual agreement rather than direct control.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment
If approved, the following is provided as feedback to the NERC SDT that will be addressing the SAR: Southern Company suggests the SDT consider modifying the glossary definition of EACMS and to revise the Supply Chain Reliability Standards to include: (i) EACMSs, specifically those systems that provide electronic access control (**excluding monitoring and logging**) to high and medium impact BES Cyber Systems; and (ii)PACSs that provide physical access control (**excluding alarming and logging**) to high and medium impact BES Cyber Systems, if PACS is to be added.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	

Comment

Reclamation recommends CIP-013 be revised to allow entities to implement a single process for procuring products and services associated with all impact levels of their BCS as well as all applicable systems (EACMS, PACS, PCAs, etc.). To achieve this, Reclamation recommends allowing entities to apply CIP-013-1 procurement protections to their low impact systems. Having the standard only apply to high and medium impact BCSs and their applicable systems could introduce risk through the unmanaged CIP-013-1 procurement portions of those systems that also support low impact BCS.

If low impact BCS are included in the scope of CIP-013, Reclamation recommends the standard allow entities to make a risk-based decision to purchase and implement a product in the absence of that product's vendor being able to meet the entity's requirements (e.g., R1.2.1 through R1.2.6).

Reclamation recommends the objectives for ensuring supply chain security throughout the procurement process not be left to choice as this will cause inconsistency across the industry. Therefore, Reclamation recommends NERC investigate existing supply chain risk management standards (e.g., National Institute of Standards and Technology, Federal Acquisition Supply Chain Security Act of 2018, and Section 889 of the National Defense Authorization Act for Fiscal Year 2019) and align CIP-013-1 with those requirements.

Reclamation recommends the revised CIP-013 standard include procurement protections of routable components for low impact BCSs, EACMS, PACS, and PCAs. The SAR should include procurement protections for EACMS, PACS, PCAs commensurate with the highest level of BES Cyber System managed by each PACS.

Finally, Reclamation recommends a 24-month implementation period for entities to comply with the revised high and medium impact portions of CIP-013 and a 48-month implementation period for entities to comply with any new low impact requirements.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	
Document Name	

Comment

Would associated EACMS and PACS be brought in-scope for CIP-005-6 R2 and CIP-010-3 R1.6? Please address exceptions for open source or free software not provided by the vendor but needed for operations (Putty, Wireshark, etc.). Please address whether the standard necessitates an asset management system to link Cyber Assets and software to the contract they are procured under. Will CIP Exceptional Circumstances be considered for Cyber Assets and software procured for emergencies?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	
Document Name	
Comment	
Dominion Energy agrees with EEI's additional comments, specifically: 1. That NERC provide a link to the May 17, 2019, Cyber Security Supply Chain Risks Staff Report and Recommended Actions within the SAR since this report is being used to set the boundaries that will be used by the SDT when addressing modifications to PACSs. While the report is mentioned within the SAR, we believe tighter linkage to this report would be beneficial, and 2. That language be added to the SAR Scope to include acknowledging the need for on-going coordination between the Project 2016-02 and Project 2019-03 SDTs. Given the overlapping project efforts, we believe it is important that both SDTs remain aligned throughout the life of each project.	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	
Document Name	
Comment	
PG&E provides no additional comments.	
Likes 0	
Dislikes 0	

Response
Leanna Lamatrice - AEP - 3,5
Answer	
Document Name	
Comment
The exclusion of these systems was discussed heavily during the drafting of the standards. It is AEP's belief that if these systems are not included in the standard we are leaving a significant opening for an attacker.
Likes 0	
Dislikes 0	
Response
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper
Answer	
Document Name	
Comment
No comments.
Likes 0	
Dislikes 0	
Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2019-03 Cyber Security Supply Chain Risks SAR Drafting Team

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2019-03 Cyber Security Supply Chain Risks** SAR drafting team (SDT) members by **8 p.m. Eastern, Thursday, August 1, 2019.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Cyber Security Supply Chain Risks

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 directing NERC to develop modifications to the Supply Chain Standards. FERC directed NERC to submit modifications to address EACMSs, specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850. In addition, NERC also recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. The modifications to address PACS do not have a regulatory deadline, but will be addressed by this project.

Standards affected: CIP-005-6, CIP-010-3, and CIP-013-1

A significant time commitment is expected of review and drafting team members to meet the regulatory deadline established in Order No. 850. Review and drafting team activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately one face-to-face meeting per quarter can be expected (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the drafting team sets forth. NERC is seeking individuals who have significant management experience or subject matter expertise with the global supply system related to communications and control hardware, software, and services affecting BES operations and BES Cyber Systems. There is a need for a team member(s) with an understanding of procurement practices for BES Cyber Assets, with a focus on cyber security. Expertise with developing

and implementing controls, including policies, practices, guidelines, and standards designed to mitigate the introduction of cybersecurity risks in the supply chain is needed.

Name:	
Organization:	
Address:	
Telephone:	
Email:	
Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):	
If you are currently a member of any NERC drafting team, please list each team here: ☐ Not currently on any active SAR or standard drafting team. ☐ Currently a member of the following SAR or standard drafting team(s):	
If you previously worked on any NERC drafting team please identify the team(s): ☐ No prior NERC SAR or standard drafting team. ☐ Prior experience on the following team(s):	

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ Texas RE	☐ NPCC	☐ WECC
☐ FRCC	☐ RF	☐ NA – Not Applicable
☐ MRO	☐ SERC	

Select each Industry Segment that you represent:

☐	1 — Transmission Owners

☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	
Name:		Telephone:	
Organization:		Email:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Nomination Period Open through August 1, 2019

Now Available

Nominations are being sought for SAR drafting team members through **8 p.m. Eastern, Thursday, August 1, 2019**.

Use the electronic form to submit a nomination. If you experience any difficulties using the electronic form, contact Linda Jenkins. An unofficial Word version of the nomination form is posted on the Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be one face-to-face meeting per quarter (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed upon timeline the team sets forth. Team members may also have side projects, either individually or by sub-group, to present for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful ballot.

Previous drafting team experience is beneficial but not required. See the project page and unofficial nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the SAR drafting team in August 2019. Nominees will be notified shortly after they have been appointed**.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to Cyber Security – Supply Chain Controls Standard		
Date Submitted:	June 26, 2019		
SAR Requester			
Name:	Soo Jin, Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☒ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. In this order FERC also directed NERC to develop modifications to the Supply Chain Standards. In addition, NERC published a Cyber Security Supply Chain Risks report on May 17, 2019 with recommendations for additional modifications to the Supply Chain Standards.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the directives issued by FERC in Order No. 850 to modify the Supply Chain Standards. The drafting team will also consider the recommendations from NERC staff's Cyber Security Supply Chain Risks report published on May 17, 2019.			

Requested information
Project Scope (Define the parameters of the proposed project):
This project will address the directives issued by FERC in Order No. 850. This project will also consider NERC staff recommendation from the Supply Chain Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
Revise the Supply Chain Reliability Standards to include: (i) EACMSs, to high and medium impact BES Cyber Systems; (ii) consideration of the recommendations in the Supply Chain Risks Report; and (iii) coordination with the Project 2016-02 team specifically around the proposed definition changes such as EACMS, BES Cyber Asset, Virtual Cyber Asset, etc. These proposed definitions could have direct impacts to the Supply Chain Reliability Standards through possible scope expansion. FERC directed NERC to submit modifications to address EACMSs to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions.
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to Cyber Security – Supply Chain Controls Standard		
Date Submitted:	June 26, 2019		
SAR Requester			
Name:	Soo Jin, Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☒ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. In this order FERC also directed~~ing~~ NERC to develop modifications to the Supply Chain Standards. In addition, NERC published a Cyber Security Supply Chain Risks report on May 17, 2019 ~~and~~ with recommendations for additional modifications to the Supply Chain Standards.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the directives issued by FERC in Order No. 850 to modify the Supply Chain Standards. ~~FERC directed NERC to submit modifications to address EACMSs, specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850.~~ The drafting team will also consider the recommendations from NERC staff's Cyber Security Supply Chain Risks report published on May 17, 2019. ~~In addition, NERC also recommends revising the Supply~~			

Requested information
~~Chain Standards to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. The modifications to address PACS do not have a regulatory deadline, but will be addressed by this project.~~
Project Scope (Define the parameters of the proposed project):
This project will address the directives issued by FERC in Order No. 850. This project will also ~~address~~ consider NERC staff recommendation from the Supply Chain Report. This team will work to coordinate with other ongoing CIP development projects ~~Project 2016-02~~ to ensure alignment with any changes to definition or standards and requirements. ~~to address Physical Access Control Systems (PACS) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.~~
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
~~Consider recommendations to R~~revise the Supply Chain Reliability Standards to include: (i) EACMSs, ~~specifically those systems that provide electronic access control (excluding monitoring and logging)~~ to high and medium impact BES Cyber Systems; ~~and~~ (ii) consideration of the ~~recommenations~~recommendations in the Supply Chain Risks Report; and~~PACSs that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems~~(iii) ~~.~~ coordination with the Project 2016-02 team specifically around the proposed definition changes such as ~~around~~ EACMS, BES Cyber Asset, Virtual Cyber Asset, etc.~~.~~ These proposed definitions could have direct impacts to the Supply Chain Reliability Standards through possible scope ~~expanision~~expansion. FERC directed NERC to submit modifications to address EACMSs~~, specifically those systems that provide electronic access control~~ to high and medium impact BES Cyber Systems. FERC directed NERC to submit the modified Reliability Standard including the directed revisions for approval within 24 months from the effective date of Order No. 850.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time. ~~However, a question will be asked during the SAR comment period to ensure all aspects are considered.~~
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.* Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.* Transmission

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP Standards for changes to ~~defintions~~definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions.
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	1. High Impact BES Cyber Systems and their associated:PCA; 2. PACS; and 3. EACMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. PCA; 2. PACS; and 3. EACMS	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System. • PACS or EACMS Methods to disable active vendor remote access either through electronic access point, an intermediate system or any other method of remote acess

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions for PACS (2.4); or one or more methods to disable active vendor remote access for PACS (2.5).	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions, excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access,

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5). OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions for PACS (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access for PACS (including Interactive Remote Access and system-to-system remote access) (2.5).	excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.

- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7~~6~~

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7~~6~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 201~~6~~-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" ~~-~~The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). ~~-~~Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. ~~-~~Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. ~~-~~For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7~~6~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7~~6~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7~~6~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7~~6~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7~~6~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. PCA; 2. PACS; and ~~1.~~3. EACMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. PCA; 2. PACS; and ~~1.~~3. EACMS	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7~~6~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and ~~1.~~3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and ~~1.~~3. PCA ~~PCA~~	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System. • PACS or EACMS Methods to disable active vendor remote access either through electronic access point, an intermediate system or any other method of remote acess

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~ CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions for PACS (2.4); or one or more methods to disable active vendor remote access for PACS (2.5).	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions, excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access,

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5). OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions for PACS (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access for PACS (including Interactive Remote Access and system-to-system remote access) (2.5).	excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.

- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or

medium impact BES Cyber System with External Routable Connectivity except as provided in Requirement R1, Part 1.6.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be

necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in

those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:
The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007.

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:
Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a

plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would

negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient

Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber

Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for

these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-43

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~3~~4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2019-06-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. ~~-~~Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. ~~-~~The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002~~-5.1~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~-~~ Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or

medium impact BES Cyber System with External Routable Connectivity except as provided in Requirement R1, Part 1.6.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-~~3~~4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-~~3~~4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). ~~-~~This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. ~~-~~Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance -that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. -Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be

necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in

those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:
The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:
The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007.

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:
Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a

plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would

negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient

Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber

Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for

these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.

R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Rationale

Note: The Rationale section has not been revised as part of the initial ballot for Project 2019-03. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

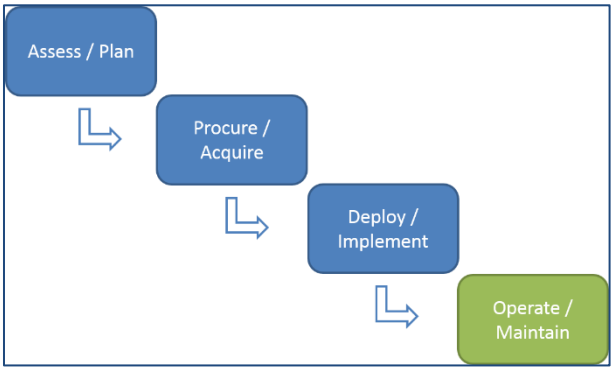
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019

Anticipated Actions	Date
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	April – May 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-21**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2~~1~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002~~-5,~~ or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 201~~6~~9-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~s~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~s~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber ~~s~~Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber ~~s~~Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber sSystems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber sSystems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber sSystems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber sSystems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.

R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Rationale

Note: The Rationale section has not been revised as part of the initial ballot for Project 2019-03. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

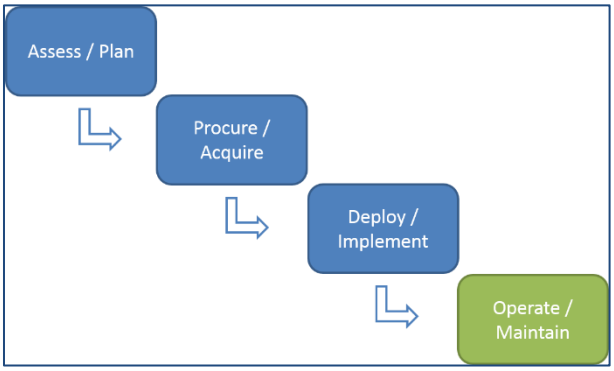
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT

- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 12 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 12 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard):

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and

categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-03 Cyber Security Supply Chain Risks

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-005-7, CIP-010-4 and CIP-013-2** by **8 p.m. Eastern, Wednesday, March 11, 2019.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

Project 2019-03 is in response to FERC Order 850 and the NERC Supply Chain Report to make modifications to the Supply Chain Standards, CIP-005-7, CIP-010-4, and CIP-013-2.

The NERC supply chain report recommended including EACMS that provide electronic access control (excluding monitoring and logging). The SDT considered excluding monitoring and logging however, operationally classifying assets using multiple definitions under different requirement of the same standard, and from standard to standard, has the potential to create confusion and unnecessary complexity in compliance programs.

The NERC supply chain report recommended including PACS (excluding alerting and logging). The Standard Drafting Team (SDT) considered excluding alerting and logging however, operationally dealing with separate functionalities within the same asset definition has the potential to create confusion within the other standards that reference the current PACS definition in the applicability column.

In conclusion, the team has decided to use the currently approved glossary definitions of EACMS and PACS in modifications to the Supply Chain Standards. The currently approved glossary definitions are all inclusive of the functionality of the systems and do not separate any subset of functions. Any modification to the existing definitions would have a wide impact on the CIP standards outside of the Supply Chain Standards.

Questions

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining **OR** disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining **AND** disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

   ☐ Yes

   ☐ No

   Comments:

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

   ☐ Yes

   ☐ No

   Comments:

5. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

6. Provide any additional comments for the standard drafting team to consider, if desired

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirement R1
The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R1
The VSL did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R2
The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R2
The VSL is explained in the following pages.

VRF Justification for CIP-010-4
The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4
The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2, Requirement R1
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R1
The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words “and their associated EACMS and PACS” were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R2
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R2

The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R3
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R3
The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions for PACS (2.4); or one	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions,

	or more methods to disable active vendor remote access for PACS (2.5).	Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5). OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions for PACS (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access for PACS (including Interactive Remote Access and system-to-system remote access) (2.5).	excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access, excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from the FERC approved CIP-005-6 Reliability Standard, with the following exceptions. In the moderate VSL, a new level is added for the violation of not having "method(s) for determining active vendor remote access sessions for PACS (2.4); **or** one or more methods to disable active vendor remote access for PACS (2.5)." In the high VSL, a new level is added for not having "one or more method(s) for determining active vendor remote access sessions for PACS (including Interactive Remote Access and system-to-system remote access) (2.4) **and** one or more methods to disable active vendor remote access for PACS (including Interactive Remote Access and system-to-system remote access) (2.5). These additions are made to reflect the addition of PACS to the applicable systems column for this requirement and reflect the risk PACS pose. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirements R2.4 and R2.5 and CIP-010-4 Requirement R1.6 and to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirements R2.4 and R2.5 and CIP-010-4 Requirement R1.6 and to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through March 11, 2020
Ballot Pools Forming Through February 25, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Wednesday, March 11, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Tuesday, February 25, 2020.** Registered Ballot Body members can join the ballot pools here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 2-11, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify "Project 2019-03 Cyber Security Supply Chain Risks Observer List" in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2
Comment Period Start Date:	1/27/2020
Comment Period End Date:	3/11/2020
Associated Ballots:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 IN 1 ST

There were 66 sets of responses, including comments from approximately 137 different people from approximately 96 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

5. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

6. Provide any additional comments for the standard drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC

					Jennifer Brey	Arizona Electric Power Cooperative	1	WECC
					Joseph Smith	Prairie Power , Inc.	1,3	SERC
					Steven Myers	North Carolina EMC	3,4,5	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC

					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC

David Kiguel	Independent	7	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Mike Forte	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Quintin Lee	Eversource Energy	1	NPCC

					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
Lower Colorado River Authority	Teresa Cantwell	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	No
Document Name	

Comment

The risk focus should be limited to controls only, not monitoring.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

NO. Changes to these Standards are not needed at all!

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Changes to these Standards are not needed at all!

Likes 0	
Dislikes 0	

Response	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Changes to these standards are not needed at all.	
Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	

We agree with the addition of EACMS (and PACS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of EACMS (and PACS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

EACMS are currently defined as:

“Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.”

EACMS are tied to ESPs. ESPs only exist with respect to Medium Impact BES Cyber Systems connected using a routable protocol. EACMS monitor and control the EAP on an ESP, so only Medium Impact BES Cyber Systems with External Routable Connectivity apply.

We understand that Applicable Systems cannot simply be changed to “Medium Impact BES Cyber Systems with External Routable Connectivity” because that would take Medium Impact BES Cyber Systems out of scope.

We recommend, for clarity and consistency among CIP standards:

Insert:

“Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS”

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes there is the potential for the definitions and requirements to be in conflict with Project 2016-02, specifically where Project 2016-02 is working on definitions of EACMS vs EACS/EAMS to address different risk and security architecture in a virtualized environment. Project 2016-02 should be permitted to finish the work and have a planned implement date prior to another revision being implemented.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E agrees with the addition of EACMS but does not agree with the use of EACMS as currently defined in the “Applicable System Columns in Tables” section of the Standard. Including EACMS which provides “access control”, “monitoring”, and “alerting” capabilities extend what FERC indicated in Order 850 which indicated only “access control”. PG&E believes the risk of EACMS which “only” provides monitoring and alerting capabilities is not the same as those which provide “access control” and should be excluded from the Standard. PG&E does indicate if an EACMS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard. PG&E recommends the definition in the “Applicable System Columns in Tables” section be altered to indicate only those EACMS which provide “access control” and that EACMS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of EACMS would be covered with examples to help clarify any confusion. A potential benefit in making the “Applicable Systems Column in Table” indicate EACMS with only “access control” is to the Project 2016-02 SDT working on the separation of EACMS into Cyber Assets for “access control” (EACS) and monitoring/alerting (EAMS). A clear indication of “access control” in the Project 2019-03 modifications could make it easier for the Project 2016-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the EACMS separation.	
Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	

Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements. The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit.	
Likes 0	
Dislikes 0	

Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Although the CAISO acknowledges that EACMS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this	

project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports EEI comments on this question. In addition, Xcel Energy suggests adding the following language after EACMS in that applicability column of CIP-005-6 R2.4 and R2.5, CIP-010-4 and CIP-013-2 "***that perform the function of controlling electronic access****."* Xcel Energy believes that this language would bring into scope all systems the perform access controls at an ESP, while excluding systems that only perform monitoring and or logging.

Making this change is supported by the Commission in Order 850 P55, where they state that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." The limitation of EACMS is also supported by NERC in the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9 that "upon evaluation of the supply chain-related risks associated with EACMSs, particularly those posed by compromise of electronic access functions, NERC staff recommends that the Supply Chain Standards be modified to include EACMSs that perform electronic access control for high and medium BES Cyber Systems."

The addition of EACMS that only perform logging and monitoring access to the Supply Chain Standards, especially CIP-005-6 R2.4 and R2.5, would likely cause additional operational costs and significant admirative burden on systems that both FERC and NERC have indicated are not of equal risk to the BPS as those systems that are performing access controls to an ESP.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb

Answer	No
Document Name	

Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 1.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding EACMS and Intermediate Systems.While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding EACMS and Intermediate Systems.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	No
Document Name	

Comment

Overall, Southern DOES NOT agree with the addition of EACMS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDT needs to address the scenario of terminating vendor remote access to the (EACMS) assets that are used to allow and prevent vendor remote access. In essence, if I must only allow vendor remote access through an authorized and authenticated session at an EACMS, and that EACMS is the asset I would use to prevent vendor remote access to a BCS, how then can I also prevent vendor remote access to that very asset that I use to terminate that remote access? This results in illogical loop. Also consider how to handle situations where a vendor is managing EACMS on behalf of the entity where disabling access to access controls seems causes that type of an illogical loop.

FERC has not ordered adding EACMS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on risk that could apply to EACMS. We agree with the FERC Order that there should be additional requirements for those EACS assets that perform “access control” functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for EACMS to clarify the difference between EACS and EAMS, we do not agree with the addition of EACMS at this time as the current definition of EACMS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report.

For these reasons, keeping requirements applicable to EACMS in CIP-010 and CIP-013 addresses the FERC Order, however Southern believes the SDT should remove EACMS from CIP-005 R2.4 and R2.5 until such time that the EACMS definition can be modified and new definitions of applicable systems be added to properly scope these requirements, and the SDT can address the infinite loop issues addressed above.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3

Answer	No
Document Name	

Comment

Tampa Electric supports EEI comments which supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that “the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard.” (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only “revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.” (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.

Likes 0	

Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	

Comment
CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	

Comment
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column. Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No

Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees with adding EACMS to the Supply Chain Standards as currently described above.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG supports RSC comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree conceptually with including EACMS but need to assess the risk and implementation.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC respectfully reiterates the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, MPC continues to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, MPC also has concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" MPC respectfully suggest that the ERO Enterprise and the SDT consider the codependent nature of these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only "revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems." (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.

Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
We agree conceptually with including EACMS but need to assess the risk and implementation. We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	

Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column.	

Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC

Answer	No
Document Name	

Comment

We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS.

There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure.

Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?

Another issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I'm not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern DOES NOT agree with the addition of PACS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDTs has now inadvertently brought into scope corporate systems and applications that do not meet the defined terms of an Applicable System. Since PACS are not required to be in an ESP, and remote access to them is not required to traverse through an Intermediate System, then there is no existing outer boundary used for remote access to PACS assets that is in-scope. FERC has not ordered adding PACS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on risk that could apply to PACS. We agree with the FERC Order and the NERC Study that there should be additional requirements for those PACS assets that perform "access control" functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for PACS to clarify the difference between PACS and PAMS, we do not agree with the addition of PACS at this time as the current definition of PACS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report. For these reasons, keeping requirements applicable to PACS in CIP-010 and CIP-013 addresses the FERC Order and NERC Study, however Southern believes the SDT should remove PACS from CIP-005 R2.4 and R2.5 until such time that the PACS definition can be modified and new definitions of applicable systems be added to properly scope these requirements.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree with the addition of PACS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding PACS and Intermediate Systems.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD believes that the PACS should not be added per the following discussion.

The Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommended that PCAs be excluded from CIP-013-2 because 1) the risk is difficult to quantify and 2) there is not a direct 15-minute impact related to the PCA itself. The PCAs were excluded from CIP-010 and CIP-013, but included a recommendation to address them as a best practice.

PCAs, like PACS, have no direct 15-minute BES impact. PACS, unlike PCAs, do not reside within an ESP and have no network access to the BCS or related ESP. Therefore; if PCAs are not included, it seems logical for PACS to be treated in the same manner.

The NERC Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) reasoned that PCA could be excluded from CIP-010 and CIP-013 due to the following:

1. *"The potential risk can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards and others which can be addressed in policies and procedures. For example, implementing access control lists, intrusion prevention systems, and malicious software prevention tools can be used to limit the risk posed by PCAs possibly impacting interconnected BES Cyber Systems" (p. 21).*

2. *The recommendation was to not include PCAs as "other controls deployed on the BES Cyber Systems under the CIP-007 and CIP-010 standards would protect the actual assets that could have a 15-minute impact if rendered unavailable, degraded, or misused" (p. 22).*

In conclusion, CHPD agrees with the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommendation to exclude PCAs in favor of a best practice approach and adequate cyber security controls. CHPD recommends that this same reasoning be extended to PACS due to the lower potential risk to the BES.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC's conclusion in Chapter 3 of the Supply Chain Risks report that "*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*" because the conclusion is inconsistent with the current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined "[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System****. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.*" Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify cyber assets that "…. control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers," such cyber assets are appropriately classified as PACS. Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT's acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

It’s not clear what risk this is mitigating. Critical sites have additional protections (security guards) that are in place and will continue to provide visibility where needed in the event someone obtains unauthorized remote access to PACS.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including

findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We agree conceptually on the intent but wonder if there is a real benefits on the overall electric reliability.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

1. The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. This leads to confusion when identifying and developing procedures for cyber assets in or out of scope, when determining compliance to the standard, and at audits or when processing risk, cause, corrective and enforcement actions.

Recommend either removing the references in all revisions or revise the SAR to include a separate class of Cyber Systems which perform either the preventive control (IPS, Firewalls) or detective control functions (IDS, logging and alerting)

2. The "Applicable Systems" language does not distinguish between medium EACMS and PACS with ERC, however ERC is a consideration when classifying systems in the Parts.

Recommend initiating a revision to the Applicable Systems and Parts to address only a) EACMS and PACS with ERC as follows:

"Physical Access Control Systems (PACS) with External Routable Connectivity – Applies to each Physical Access Control System with ERC and associated with a referenced high impact or medium impact BES Cyber System"

"Electronic Access Control or Monitoring Systems (EACMS) with External Routable Connectivity – Applies to each Electronic Access Control or Monitoring System with ERC and associated with a referenced high or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems."

3. CIP-010-4 – "Applicable Systems" – PACS (pp5-6) includes for PACS "except as provided in Requirement R1, Part 1.6." This is confusing and potentially adds Cyber Systems into scope which are not in scope

Recommend updating the Applicable Systems definitions to match the Parts where ERC is or is not required.

4. CIP-010-4 Part R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE agrees conceptually with including PACS but needs to assess the risk and implementation. However, we expect a lower return on investment on PACS.

There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure.

Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?

We agree with the proposed changes. *We do see one issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I'm not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1*

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	

Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy does not oppose the addition of PACS, but agrees with the NSRF that consideration and clarity is needed around Medium Impact BES Cyber Systems with and without External Routable Connectivity.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E agrees with the addition of PACS but does not agree with the use of PACS as currently defined in the “Applicable System Columns in Tables” section of the Standard. Including PACS which only provide monitoring or alerting capabilities in the modifications extends what was indicated in the NERC supply chain study recommendation which indicated only “access control” capabilities. PG&E believes the risk of PACS which “only” provides monitoring and alerting capabilities is not the same as those which provide “access control” capabilities and should be excluded from the Standard. PG&E does indicate if a PACS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard. PG&E recommends the definition in the “Applicable System Columns in Tables” section be altered to indicate only those PACS which provide “access control” and that PACS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of PACS would be covered with examples to help clarify any confusion. A potential benefit in making the “Applicable Systems Column in Table” indicate PACS with only “access control” is to the Project 2016-02 SDT working on the separation of PACS into Cyber Assets for “access control” (PACS) and monitoring/alerting (PAMS). A clear indication of “access control” in the Project 2019-03 modifications could make it easier for the Project 2016.-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the PACS separation.	
Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment
OPG supports RSC comments.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC's conclusion in Chapter 3 of the Supply Chain Risks report that "*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*" because the conclusion is inconsistent with the

current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined "[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System****. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.*" Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify cyber assets that "…. control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers," such cyber assets are appropriately classified as PACS. Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT's acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	

We agree with the addition of PACS (and EACMS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of PACS (and EACMS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

PACS are currently defined as:

“Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.”

PACS are tied to PSPs. PSPs only exist with respect to Medium Impact BES Cyber Systems for those with ERC per CIP-006-6 Requirement R1, Part 1.2. Medium Impact BES Cyber Systems without External Routable Connectivity are only required to define operational or procedural controls to restrict physical access; a PACS is not required.

We recommend, for clarity and consistency among CIP standards:

1.) Insert:

“Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS”

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

2.) Delete “except as provided in Requirement R1, Part 1.6” from the PACS description in the Background on p. 6.

Although the PACS applicability language does not directly affect CIP-005-7, we recommend that the new inclusion of PACS applicability in the Background on p. 6 include “with External Routable Connectivity” to be consistent with most of the standards. CIP-006-6 and CIP-007-6 should likewise be corrected during the next revision.

CIP-006-6 and CIP-007-6 language:

“Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.”

CIP-004-6, CIP-009-6, CIP-010-3 and CIP-011-2 language:

“Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.”

Also, in keeping with the same principle, for CIP-013-2, we suggest changing Requirement R1, “for high and medium impact BES Cyber Systems and their associated EACMS and PACS,” to “for high and medium impact BES Cyber Systems, and EACMS and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.”

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response
Bruce Reimer - Manitoba Hydro - 1

Answer	No

Document Name	
Comment	

We agree to add PACS to the applicable systems but disagree with the language regarding PACS in CIP-013-2 R1 and CIP-010-4 Section 6 Background since it would bring PACS associated with BCS w/o ERC into scope. Currently It has been commonly understood that only PACS associated with BCS with ERC is applicable to the CIP standards based on CIP-006 R1.1 requirement in which PACS is not required for medium impact BCS without ERC. We suggest making the following changes:

For CIP-013-2 R1, Part 1.1 and Part 1.2, change “high and medium impact BES Cyber Systems and their associated EACMS and PACS” to “high and medium impact BES Cyber Systems and their associated EACMS, and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.”

For CIP-010-4, remove the wording “except as provided in Requirement R1, Part 1.6.” from Section 6 Background.

Likes 0	
Dislikes 0	
Response	

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	

Adding PACs is not necessary. The standards as they are right now are just fine.

Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

Adding PACS is not necessary. The standards as they are right now are just fine.

Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	

The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. In addition, the Applicable Systems and language does not distinguish between EACMS and PACS with ERC. Recommend revising Definitions, Applicable Systems and Parts to address only EAMCS and PACS with ERC and which perform preventive security services.

CIP-010-4 – Applicable Systems – PACS (pp5-6): current term of a PACS "except as provided in Requirement R1, Part 1.6." adds Cyber Systems into scope which are not in scope. It is not clear and confusing.

CIP-010-4 R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	

NO. Adding PACS is not necessary. The Standards as they are right now are just fine.

Likes 0	
Dislikes 0	
Response	

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Tampa Elecric does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 2.	

Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC requests clarification. Was it the SDT's intent not to capitalize "electronic access point" and "intermediate system" under CIP-005-7, requirement R2, part 2.5, bullet three under Measures? NYISO doesn't understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with adding PACS to the Supply Chain Standards as currently described above.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	

Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. They should be low, or better yet not a violation at all.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
They should be low, or better yet not a violation at all.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
They should be low, or better yet not a violation at all.	
Likes 0	
Dislikes 0	

Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed. 1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established. We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis: "… where permitted and not otherwise blocked or unable to be established…" R2.5 can then be changed to add "according to R2.4 above" before the parenthesis. 2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions: Expand EACMS to "EACMS that provide electronic access control (excluding monitoring and logging)," or equivalent language. Expand PACS to "PACS that provide physical access control (excluding alerting and logging)"	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The wording is awkward and should be clarified to explain that failing to have one of the two methods required (determining OR disabling) is a moderate VSL while failure to have any of the required methods (lacking BOTH a means to determine and lacking a means to disable) is a high VSL.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the modified VSLs, but agrees with the NSRF that the language should be clarified for the scenario where a Responsible Entity does not permit vendor remote access sessions for some or all vendors. Alliant Energy also supports the NSRF's comments to update the applicability section to include only EACMS that provide electronic access control (excluding monitoring and logging) and PACS that provide physical access control (excluding alerting and logging).	
Likes 0	
Dislikes 0	

Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements. The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit. In support of the lower impact and risk, both VSLs should be listed as minimal to moderate.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	No
Document Name	
Comment	
Due to the low risks Vendor remote access to PACS have to the operation of the BES, we feel the VSLs should be the lowest possible. The protections and requirements already afforded to Vendor remote access to PACS: access control, PRAs, training, etc., already reduce the risks PACS pose to the BES. The new requirements are a best practice, and do not have a high enough risk level to warrant a Medium or High VSL.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Agree with Duke Energy's comment. "Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate."	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry’s supply chain security standard.	
Likes 0	

Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
If PACS was added, which I disagree with, the modified VSLs can help at the time of enforcement, but don't help during implementation. VSLs are not evaluated when determining how to implement CIP requirements and VSLs do not influence the level of effort applied to protect the BES.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed. 1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established. We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis: "… where permitted and not otherwise blocked or unable to be established…" R2.5 can then be changed to add "according to R2.4 above" before the parenthesis. 2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions: Expand EACMS to "EACMS that provide electronic access control (excluding monitoring and logging)," or equivalent language. Expand PACS to "PACS that provide physical access control (excluding alerting and logging)"	
Likes 0	

Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Based on response under question #2 above.	
Likes 0	
Dislikes 0	
Response	

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No Comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	

Answer	Yes
Document Name	
Comment	
PG&E agrees with the indicated VSL assignments for PACS.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment
Xcel Energy supports EEI comments and does not oppose the changes to VSLs.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	

Comment
NYISO doesn't understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	Yes
Document Name	

Comment
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 3.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	

Comment
CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
EEI supports the modifications made to the VSLs.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment
Southern supports the modifications to the VSL’s. However, see our comments in questions 1 and 2 with regard to the addition of EACMS and PACS assets to the scope of these new requirements.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Tampa Elecric supports the modifications made to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	

Response
Becky Webb - Exelon - 6
Answer	
Document Name	
Comment
Exelon will align with EEI's comments in response to this question.
Likes 0	
Dislikes 0	
Response
Kinte Whitehead - Exelon - 3
Answer	
Document Name	
Comment
Exelon will align with EEI's comments in response to this question.
Likes 0	
Dislikes 0	
Response

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
We would prefer an 18 month implementation to better accommodate a budget cycle	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Tampa Elecric supports EEI recommendation that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Eversource suggests an 18-month implementation plan due to current experience with adding vendors to the initial Supply Chain project.	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
We recommend a longer implementation period than the proposed 12 months.	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern recommends that the SDT expand the proposed time for implementation plan to 18 months and suggests for the SDT to consider budget cycles for possible technological upgrades needed before implementation. In this case, 18 months would be a fair alternate time frame. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

MidAmerican agrees with MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb

Answer	No
Document Name	

Comment

Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 4

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks

Answer	No
Document Name	
Comment	

The IRC SRC recommends an 18- or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they will need to develop and implement a different process for EACMS and PACS systems. Therefore, the IRC SRC requests the SDT allow additional time.

Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 4.

Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	

Xcel Energy supports EEI comments on this question and believes that an 18 month implementation period would be more appropriate.

Likes 0	
Dislikes 0	
Response	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature.

The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are embedded. Introduction of electronic access

control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity's existing program. Therefore, we strongly disagree with the assertion that the changes are administrative.

Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes.

For these reasons, GSOC and GTC recommend a 24 month implementation plan.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC does not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. Budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes. For these reasons, MPC recommends an 18 month implementation plan.

Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
Because EACMS and PACS may be located outside of any Electronic Security Perimeter (Intermediate Systems MUST be outside any ESP), N&ST believes entities *could* find it necessary to define and implement controls for CIP-005 R2.4 and R2.5 for EACMS and PACS that are entirely different than the ones they have implemented for BES Cyber Systems and PCAs. Therefore, N&ST believes the implementation plan duration should be 18 months, not 12 months.	
Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24 month implementation plan after the applicable governmental entity’s order approving the standard to allow entities flexibility to determine the appropriate implementation.	
Likes 0	
Dislikes 0	

Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The proposed implementation timeline may not allow enough time for industry to properly gauge the effects of the preceding version of standards Subject to Enforcement. Based on the outcomes of the yet to become effective versions of the Standards, additional budget and time could be needed to implement the proposed updates. SRP would like to recommend an implementation timeline of 15 to 18 calendar months, starting in the next calendar quarter of the approval of CIP-005-7, CIP-010-4, and CIP-013-2.	

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

The IRC SRC recommends an 18 or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they will need to develop and implement a different process for EACMS and PACS systems, so the IRC SRC requests the SDT allow additional time.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

Considering the scope of changes introduced by SDT, we recommend an 18 or 24 month implementation plan.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5

Answer	No
Document Name	

Comment

Entergy proposes an 18 month implementation plan as was approved via Project 2016-03 for these standards. While the requirement language does not change, the inclusion of systems that were not originally included in the Project 2016-03 scope should allow for the same timeline of implementation

as entities must again evaluate compliance strategies for new sets of hardware and/or software that may not be compatible with the entity’s expected processes for BCA and PCA assets.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	

Comment

Agree with Duke Energy's comment.

"Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards’ security objectives, which could involve a longer time-horizon, capital budgets and planning cycles."

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

18 months minimum

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Although adding the words EACMs and PACS to the requirements seems fairly innocuous. It can in fact be a significant impact to an Entity's CIP compliance program and approach. Entities may need to evaluate, procure and implement new technologies and processes to incorporate these systems.

Recommend a 24 month implementation.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with NSRF and EEI's comments recommending that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
From participation NERC and industry discussions, it appears that the basis for a 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high and medium impact BES Cyber Systems. This supposition would make it appear that it is a straightforward expansion of existing Supply Chain programs to EACMS and PACS. This is not true in all cases. Notably, the high (control center) and medium (ex. substation) impact environments are very different. CEHE suggest that 12 months is not sufficient and would like to propose a 24 month implementation plan instead.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FE recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS will result in a significant expansion in scope for both hardware and software covered under existing contracts. Entities will need to modify existing policies and processes and negotiate modified contracts with existing vendors to cover new equipment and systems. In addition, these new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, we feel additional time will be required to implement the standard.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The addition of system-to-system access will take defining and further investigation; BPA believes this is a larger change than we can accomplish in 12 months. Also, Projects 2016-02 and 2019-03 definitions and implementation dates must be reconciled.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are embedded. Introduction of electronic access	

control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity's existing program. Therefore, we strongly disagree with the assertion that the changes are administrative.

Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes.

For these reasons, GSOC and GTC recommend a 24 month implementation plan.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	

Comment

The NSRF recommends an overall 18-month implementation plan. The SDT is already changing yet to be effective Standards whereby applicable entities will need to prove compliance then add additional compliance attributes (PACS and EACMS). There may be new entities who will need to start a new portion of their compliance program to satisfy these new attributes. Recommend an 18-month implementation plan.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve a longer time-horizon, capital budgets and planning cycles.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Should be 48 months or longer.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Should be 48-months or longer.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
We propose an 18 month implementation plan in order to address change management: understand the impact to existing programs, processes and documentation, revise existing documentation, develop and implement changes and test changes for integrity.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No

Document Name	
Comment	
NO. Should be 48-months, or longer.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC reccommends the SDT modify the current implementation plan to allow entities 18 months to fully implement the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
18 month is more reasonable since 12 month will be hard for entities that have many vendors to meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	

Some smaller entities may not have the resouces or time to allocate with only a one year implementation. Typically our budgets are very tight and are set one year in advance, in October. A longer implementaiton time assures we have resouces that can be allocated through the annual budget process.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO comments.

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 5

Answer	No
Document Name	

Comment

SDG&E supports EEI's recommendation that the SDT expand the proposed time for the implementation plan to 18 months.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E agrees with the proposed 12-month implementation plan. PG&E believes the Cyber Assets being brought into scope for this modification should be able to follow the same plans and processes being developed for the BES Cyber Systems (BCS) under CIP-013-1. PG&E does not anticipate significant changes to the plans or processes would need to be done exempt for an indicating that EACMS and PACS must be covered, and believes the education of personnel handling the procurement and implementation of the Part 1.2 controls for EACMS and PACS should be able to be done within the 12-month interval.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Kinte Whitehead - Exelon - 3
Answer	
Document Name	
Comment
Exelon will align with EEI's comments in response to this question.
Likes 0	
Dislikes 0	
Response
Becky Webb - Exelon - 6
Answer	
Document Name	
Comment
Exelon will align with EEI's comments in response to this question.
Likes 0	
Dislikes 0	
Response
Cynthia Lee - Exelon - 5
Answer	
Document Name	
Comment
Exelon has aligned with EEI's comment in response to this question.
Likes 0	
Dislikes 0	
Response

Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
A scope change of applicable CIP system always cause additional compliance cost. We don't know whether the current change is cost-effective or not.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
One member entity estimated the following costs and provides a recommendation: Depending on the entity, the costs associated with the proposed changes may range between an annualized cost of $80K (80 to 100 hours per person) and $500K per entity. This does not include capital expenditures for technologies which manage vendor access, which may exceed $5M per entity. This is based on the need to: a. Develop, update and implement procedures and training for multiple departments and their personnel. b. Perform updates to existing categorization processes to ensure the identification and controls exist to meet and exceed the requirements in the revisions. c. Identify existing or implement new technologies to manage supplier or vendor remote access solutions. This includes efforts in integration and changes to systems, contracts, processes and internal compliance program metrics. Recommend utilizing existing CIP program processes to meet the requirements. For example, CIP-013 R1.5 requires software integrity in the supply chain. CIP-010 R1.6 requires software integrity. CIP-007 R2 also requires integrity in software security patches. Aligning those standards into a single meaningful standard could improve cost effectiveness.	

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

While GSOC and GTC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA supports WAPA's comment as follows:

"The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work."

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E cannot agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1 has not been completed and a full understanding of the current costs is not known. PG&E would have preferred to answer this question as “Unknown”, but the option was not available.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with the NSRF’s comments.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

NERC should perform an impact analysis as part of the SAR process. Every change impacts existing documentation and process stacks.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	

Comment

In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with extending the program to EACMS and PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors to ensure they are implemented in the most cost-effective manner. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
The FERC order states this is only an “increased paperwork burden” which I disagree with. Where does this include the actual ongoing monitoring of activity and maintaining an adequate level of training personnel across multiple parts of the power systems that know how to respond?

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment
Prior to proposing additional modifications, Reclamation recommends each SDT take additional time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities economic relief by allowing technical compliance with current standards.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment
While GSOC and GTC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No

Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

No comments

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees that the FERC directives can be executed in a cost-effective manner. There will be an undue cost and burden initially to conduct business another way by adding EACMS and PACS to CIP-005 R2.4 and R2.5. Other costs will include providing new technology if not already present to track, store, and recall the data addressing the assessments provided by CIP vendors. One suggestion would be to allow the additional time suggested in Question 4 to consider those budget cycles for any possible technology upgrades.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Re-use of existing terms is easier and more cost effective than introducing new terms and/or requirements.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past. The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!	

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4

Answer	
Document Name	

Comment

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	
Comment	
No Comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy takes no position on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	

Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 5.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
Tampa Electric takes no position as to the cost effectiveness of the proposed changes	
Likes 0	
Dislikes 0	
Response	

6. Provide any additional comments for the standard drafting team to consider, if desired.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
The proposed changes to include EACMS and PAC to the CIP-010-4 requirements seem reasonable, but will add to workload.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
Tampa Electric supports the following EEI comments: In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states “[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.”) With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access. In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you’ve entered the “hall of mirrors”). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5. EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE seeks clarification as to why PACS and EACMS were not added as applicable systems for Parts 2.1-2.3. In the scenario where a vendor is utilizing Interactive Remote Access (IRA) to a BCA or PCA, Parts 2.1-2.5 would be applicable. However, if the vendor is utilizing IRA to a PACS or EACMS, Parts 2.1-2.3 would not be applicable. This would mean no Intermediate System, no encryption, or multi-factor authentication is required. Texas RE recommends PACS and EACMS should be added.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	
Document Name	
Comment	
During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and NPCC request written clarification if mitigation will be required in CIP-013-2 R1. There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months …." However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months …."	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern's comments were detailed in Questions 1-5.	
Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states “[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.”) With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access. In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you’ve entered the “hall of mirrors”). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5. EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 6.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	
1. The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs. 2. The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of CIP-013-2 requirement R1 with the *proposed* language for CIP-011-3, requirement R1, part 1.4. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks," there is no mention of mitigation (see excerpt below):	

“One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).”

Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to “identify, assess and ***mitigate*** risks in cases where vendors store Responsible Entity’s BES Cyber System Information."

The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of this proposal with respect to mitigation:

a. Modify the language under proposed under CIP-011-3, requirement R1, part 1.4 to align with CIP-013-2, requirement R1, part 1.1 ***OR***

b. Migrate all proposed vendor-related requirements under Project 2019-02: BCSI Access Management (i.e. CIP-011-3, requirement R1, part 1.4) to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.

The IRC SRC believes the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope:

“This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements."

Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 6.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy supports EEI comments on this question. In addition, upon evaluation of the addition of EACMS to CIP-005-6 R2.4 and R2.5, Xcel Energy has recognized that the requirement may limit additional controls to address the risks the requirement part is intended to address. This situation may create additional administrative burden without the consummate benefits that could be gained through policy or procedural controls.

In CIP-005-6 R2.4 the Requirement states that a Responsible Entity (RE) shall “have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)”. In CIP-005-6 R2.5 the requirement states that a RE shall “have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).” Both requirements assume that RE have systems that have the capability of Vendor Remote Access (VRA) and that the RE allows for VRA if capability exists.

Many entities may have systems that are not capable of VRA or do not allow for VRA in their programs. Yet the requirement as written would still force a RE to implement methods to determine VRA sessions and implement methods to disable VRA sessions.

Xcel Energy believes that this issue would be eliminated by adding limited language to the Requirements that reduces the scope to only those REs that allow for VRA.

Xcel Energy proposes adding the following or similar language to achieve this goal:

CIP-005-6 R2.4:

"Where the Responsible Entity permits vendor remote access, have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)."

CIP-005-6 R2.5:

"Where the Responsible Entity permits vendor remote access, have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

Xcel Energy believes these changes can be made within the scope of the current Standard Authorization Request (SAR). In the purpose section of the SAR the Standard Drafting Team (SDT) is directed to address directives issued by FERC in Order 850 and consider NERC Staff recommendations from the NERC Staff Report. In the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9-10 that recommended actions should "include recommendations to address EACMS risks in the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk as follows:"

· "Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, include recommendations relative to coordinated controls between the entity and applicable vendors associated with CIP-005-6 (Parts 2.4 and 2.5) for managing active vendor remote access sessions to and/or through EACMS cyber asset types".

In the process of addressing risk of VRA the SDT should recognize that a VRA risk is being addressed through policy or procedural controls, which current Requirement language does not allow for. If EACMS were included in the scope of the original Supply Chain project this ambiguity in requirement language could have been addressed at that time.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment

Exelon will align with EEI's comments in response to this question.

Likes 0	

Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
There are cases where the requirements would include “BES Cyber Systems, and their associated EACMS and PACS” as Applicable Systems (such as in CIP-010-4 Part 1.6, CIP-013-2 R1, R1.1, R1.2, R1.2.5). If associated PCAs are not included, the rest of the cyber assets within an Electronic Security Perimeter are also vulnerable. For example, PCA patches may be inadvertently loaded with Trojan Horses, malicious sniffers, etc., which may affect the rest of the devices in the network – including BES Cyber Systems.	
Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	

Comment

The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs.

During discussion with a member of the SDT, the member indicated mitigation would be required for CIP-013-2 requirement R1. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks" and not mitigate them as detailed below.

"One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)."

That said, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to "identify, assess and ***mitigate*** risks" as detailed below:

"Processes to identify, assess, and ***mitigate*** risks in cases where vendors store Responsible Entity's BES Cyber System Information."

If the intent of this proposal is to require mitigation for ***all*** assets under CIP-013, requirement R1, part 1.1, the IRC SRC requests the SDT to:

- Modify the language under CIP-013-2, requirement R1, part 1.1 to mirror the language proposed under CIP-011-3, requirement R1, part 1.4 ***OR***

Migrate all proposed vendor-related requirements under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4, to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	

Comment

To prevent possible confusion we suggest that all modifications proposed for CIP-005 and CIP-010 should be documented in one CIP standard (CIP-013).

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones

Answer	
Document Name	

Comment

1. The NERC SAR for this order is poorly written and inaccurate at best. The intent of the SAR is to communicate the ask, the specifics around what is required, and citations for the basis. Recommend revising the SAT to include the specific FERC Order and NERC technical paper requirements and recommendations.

2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

We would like to thank the SDT for allowing us to comment on the proposed changes.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	

Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E agrees with the EEI input on Question 6 regarding the modification to CIP-005-7, Requirement R2, Part 2.5 creating an untenable dilemma based on how it could be interpreted. This is based on the EEI comment of: "The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall)." EEI additionally indicated that if entities are required to block all access to the EACMS by installing a separate firewall, the newly installed firewall would be an EACMS which would then need to have another firewall installed creating an endless loop of new obligations.	

While the EEI recommendation indicates to remove EACMS from the Applicability Section of Requirement R2, Part 2.5, PG&E believes this would result in the modification not meeting FERC's directive in Order 850.

PG&E recommends the Requirement language be modified to indicate the endless loop condition is not the intended purpose of the modification, or guidance be created which clearly indicates it is not the intended purpose of the Requirement. The preferred solution is Requirement language since Audit Teams are not bound to the wording in guidance.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	
Document Name	

Comment

FirstEnergy urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	
Document Name	

Comment

CEHE supports the additional comments as submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment
During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and TFIST request written clarification if mitigation will be required in CIP-013-2 R1. There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months …." However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months …."

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	
Document Name	

Comment
OPG supports RSC comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment
Why are Protected Cyber Asset (PCA) or Protected Cyber System (PCS) per CIP [Definitions: Project 2016-02 Modifications to CIP Standards] not considered; given that the "impact rating of the PCA [or PCS] is equal to the highest rated BCS in the same ESP?

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	

Document Name	

Comment

Comments:

1.) Recommend the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02, i.e. CIP-011-3, requirement R1, part 1.4, “to identify, assess, and mitigate risks in cases where vendors store Responsible Entity’s BES Cyber System Information,” would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below, showing the divergence in language between the two SDTs.

2.) A SDT member indicated in conversation that mitigation would be required for CIP-013-2 requirement R1. The current language of CIP-013-2, R1, part 1.1, only requires an entity to “identify and assess cyber security risks;” there is no mention of mitigation.

Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has proposed language for CIP-011-3, requirement R1, part 1.4, that will require an entity to

implement one or more documented information protection program(s) including “Processes to identify, assess, and mitigate risks in cases where vendors store Responsible Entity’s BES Cyber System Information.”

We request the SDT, in order to avoid duplication of requirements across multiple standards, to collaborate with the SDT for Project 2019-02 to either:

- Migrate all vendor-related requirements currently proposed under CIP-011-3, R1, Part 1.4 to CIP-013-2,

OR

- Drop any plans to introduce mitigation in CIP-011-3, R1, Part 1.4 and defer to the language in the existing, similar requirement under CIP-013-1, R1, Part 1.1.

We believe the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope:

“This project will address the directives issued by FERC in Order No. 850. This project will also consider NERC staff recommendation from the Supply Chain Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements.”

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	
Document Name	

Comment

Duke Energy suggests the following:

Current CIP standards don't require entity to go beyond ESP boundary to monitor vendor remote access. Since all EACMS and PACS system don't reside within an ESP, the focus of this standard will shift beyond ESP boundary, where will be required to monitor and possibly terminate such access before such traffic even gets to ESP firewall. Duke Energy believes only EACMS or PACS devices that reside within an ESP should be the focus of this standard, so original intention of CIP-005 protection at the ESP level doesn't get derailed.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	
Document Name	

Comment

We suggest moving revised CIP-011-2 R1.4 to CIP-013 R1.1 to address BCSI cloud services provider's risks since it really belongs to the supply chain risk management.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4

Answer	
Document Name	

Comment

FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	
Document Name	

Comment

I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

1. The NERC SAR for this order is poorly written please revise to include the FERC Order and NERC technical paper requirements

2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	

Comment

I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2
Comment Period Start Date:	1/27/2020
Comment Period End Date:	3/11/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 IN 1 ST

There were 66 sets of responses, including comments from approximately 137 different people from approximately 96 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

5. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

6. Provide any additional comments for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Jennifer Brey	Arizona Electric Power Cooperative	1	WECC
					Joseph Smith	Prairie Power , Inc.	1,3	SERC
					Steven Myers	North Carolina EMC	3,4,5	SERC
					Shari Heino	Brazos Electric Power	5	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
of Chelan County					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	5	NPCC
					Mike Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Randy MacDonald	NB Power Corporation	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
Lower Colorado River Authority	Teresa Cantwell	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC's justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The risk focus should be limited to controls only, not monitoring.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Changes to these Standards are not needed at all!	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Changes to these Standards are not needed at all!	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Changes to these standards are not needed at all.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	

We agree with the addition of EACMS (and PACS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of EACMS (and PACS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

EACMS are currently defined as:

"Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

EACMS are tied to ESPs. ESPs only exist with respect to Medium Impact BES Cyber Systems connected using a routable protocol. EACMS monitor and control the EAP on an ESP, so only Medium Impact BES Cyber Systems with External Routable Connectivity apply.

We understand that Applicable Systems cannot simply be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity" because that would take Medium Impact BES Cyber Systems out of scope.

We recommend, for clarity and consistency among CIP standards:

Insert:

"Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS"

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes there is the potential for the definitions and requirements to be in conflict with Project 2016-02, specifically where Project 2016-02 is working on definitions of EACMS vs EACS/EAMS to address different risk and security architecture in a virtualized environment. Project 2016-02 should be permitted to finish the work and have a planned implement date prior to another revision being implemented.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E agrees with the addition of EACMS but does not agree with the use of EACMS as currently defined in the "Applicable System Columns in Tables" section of the Standard. Including EACMS which provides "access control", "monitoring", and "alerting" capabilities extend what FERC indicated in Order 850 which indicated only "access control". PG&E believes the risk of EACMS which "only" provides monitoring and alerting capabilities is not the same as those which provide "access control" and should be excluded from the Standard. PG&E does indicate if an EACMS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard. PG&E recommends the definition in the "Applicable System Columns in Tables" section be altered to indicate only those EACMS which provide "access control" and that EACMS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of EACMS would be covered with examples to help clarify any confusion. A potential benefit in making the "Applicable Systems Column in Table" indicate EACMS with only "access control" is to the Project 2016-02 SDT working on the	

separation of EACMS into Cyber Assets for “access control” (EACS) and monitoring/alerting (EAMS). A clear indication of “access control” in the Project 2019-03 modifications could make it easier for the Project 2016-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the EACMS separation.	
Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT	

considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.

In addition, the SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements. The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

Although the CAISO acknowledges that EACMS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC respectfully reiterate the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, GSOC and GTC continue to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, GSOC and GTC also have concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" GSOC and GTC respectfully suggest that the ERO Enterprise and the SDT consider interdependencies between these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	No
Document Name	
Comment	

Xcel Energy supports EEI comments on this question. In addition, Xcel Energy suggests adding the following language after EACMS in that applicability column of CIP-005-6 R2.4 and R2.5, CIP-010-4 and CIP-013-2 "***that perform the function of controlling electronic access.***" Xcel Energy believes that this language would bring into scope all systems the perform access controls at an ESP, while excluding systems that only perform monitoring and or logging.

Making this change is supported by the Commission in Order 850 P55, where they state that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." The limitation of EACMS is also supported by NERC in the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9 that "upon evaluation of the supply chain-related risks associated with EACMSs, particularly those posed by compromise of electronic access functions, NERC staff recommends that the Supply Chain Standards be modified to include EACMSs that perform electronic access control for high and medium BES Cyber Systems."

The addition of EACMS that only perform logging and monitoring access to the Supply Chain Standards, especially CIP-005-6 R2.4 and R2.5, would likely cause additional operational costs and significant admirative burden on systems that both FERC and NERC have indicated are not of equal risk to the BPS as those systems that are performing access controls to an ESP.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	No
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any	

confusion that may exist surrounding EACMS and Intermediate Systems.While we agree with the addition of EACMS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding EACMS and Intermediate Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:	

CIP-007-6: Requirement R2 Parts 2.1, 2.2, and 2.3, Requirement R3 Parts 3.1, 3.2, and 3.3, Requirement R4 Part 4.1, Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5 CIP-009-6: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5 CIP-010-3: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4 Requirement R3 Parts 3.1 and 3.4, CIP-011-2: Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Overall, Southern DOES NOT agree with the addition of EACMS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDT needs to address the scenario of terminating vendor remote access to the (EACMS) assets that are used to allow and prevent vendor remote access. In essence, if I must only allow vendor remote access through an authorized and authenticated session at an EACMS, and that EACMS is the asset I would use to prevent vendor remote access to a BCS, how then can I also prevent vendor remote access to that very asset that I use to terminate that remote access? This results in illogical loop. Also consider how to handle situations where a vendor is managing EACMS on behalf of the entity where disabling access to access controls seems causes that type of an illogical loop.

FERC has not ordered adding EACMS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on risk that could apply to EACMS. We agree with the FERC Order that there should be additional requirements for those EACS assets that perform "access control" functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for EACMS to clarify the difference between EACS and EAMS, we do not agree with the addition of EACMS at this time as the current definition of EACMS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report.

For these reasons, keeping requirements applicable to EACMS in CIP-010 and CIP-013 addresses the FERC Order, however Southern believes the SDT should remove EACMS from CIP-005 R2.4 and R2.5 until such time that the EACMS definition can be modified and new definitions of applicable systems be added to properly scope these requirements, and the SDT can address the infinite loop issues addressed above.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide. The illogical

loop can be solved by removing access to that EACMS itself by whatever means access is granted. The requirements do not require an EACMS to provide access to other EACMS. Please reference the draft implementation guidance for an example.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Tampa Electric supports EEI comments which supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only "revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems." (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No

Document Name	
Comment	
CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column. Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and agrees that Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) are part of the definition of Interactive Remote Access (IRA), however, ESP and EAP are only used in the definition to determine where access begins: "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)." Since a vendor remote access originates from a Cyber Assets that is outside an Entity's ESP and is not at a defined EAP, then any remote access meets the definition of IRA. The definition goes on to include places remote access may be initiated from "1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors or consultants."	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	

Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within: CIP-007-6: Requirement R2 Parts 2.1, 2.2, and 2.3, Requirement R3 Parts 3.1, 3.2, and 3.3, Requirement R4 Part 4.1, Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5	

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO comments.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4, CIP-011-2: Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with adding EACMS to the Supply Chain Standards as currently described above.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree conceptually with including EACMS but need to assess the risk and implementation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC respectfully reiterates the cooperative sector's comments in response to the Commission's Notice of Proposed Rulemaking regarding the dearth of reliability benefit associated with inclusion of those assets that provide only monitoring and logging functions and capabilities. Review of the proposed revisions, however, confirms that they meet the FERC directive set forth in Order 850. For the reasons cited in previous comments, MPC continues to have reservations regarding the reliability benefit that the application of the CIP-013, CIP-005, and CIP-010 requirements to electronic access monitoring systems would contribute. Moreover, MPC also has concerns regarding: (1) the synergies between this project and other standards development projects that are evaluating the current definition of EACMS and (2) the reconciliation of the implementation of the directive with findings presented by NERC Staff in the NERC Supply Chain report "*to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.*" MPC respectfully suggest that the ERO Enterprise and the SDT consider the codependent nature of these efforts and evaluate opportunities to better integrate them to ensure that future standards and definition modifications do not beget the need for cyclical, periodic revisions to reconcile each new set of revisions proposed by these different, but inter-dependent projects.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for	

this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide. The 2019-03 team has consulted with the 2016-02 team and believe the work we had done within our FERC deadline and does not conflict or impact the other teams work.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the addition of EACMS and agrees that modifications to the supply chain standards to address EACMS and specifically controls for ensuring reliability and security as stated in FERC Order 850 at P47 is appropriate. The Commission stated that "the standard drafting team that is formed in response to our present directive may determine…what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standard." (Order 850 at P55) We also note that in the NERC Cyber Security Supply Chain Risks Report dated May 17, 2019; it recommended only "revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems." (Chapter 2, Overview, P7) Hence, the Commission has provided the Standards Drafting Team sufficient latitude, within FERC Order 850, to focus the scope of EACMS based on supporting analysis.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	

Answer	Yes
Document Name	
Comment	
We agree conceptually with including EACMS but need to assess the risk and implementation. We agree conceptually on the intent but we think that there is a need to better define the requirements. The added requirements are in the IRA section of CIP-005 R2, one could think that for accessing the EACMS an Intermediate system is required.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT	

considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “EAMCS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	

Response
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	

Response
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EAMCS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

2. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

SDT General Response to PACS Inclusion

The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.

The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the “Background” section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3, Requirement R3 Parts 3.1, 3.2, and 3.3, Requirement R4 Part 4.1, Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5 CIP-009-6: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5 CIP-010-3: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4 Requirement R3 Parts 3.1 and 3.4, CIP-011-2: Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
While the addition of PACS and EACMS may appear to meet the spirit of the FERC Order, the addition of these two device types to CIP-005 R2 Parts 2.4 and 2.5 poses a challenge. Interactive Remote Access relies on the presence of an Electronic Security Perimeter or an Electronic Access Point, neither of which is a requirement that applies to PACS or EACMS. In its current form, the addition of PACS and EACMS to CIP-005 R2 Parts 2.4 & 2.5 would only apply to system-to-system vendor remote access, and not vendor interactive remote access. There is more work to be done to include the intended target of IRA when adding PACS and EAMCS to the applicability column. Suggest either update the definition of IRA or remove the capitalization from the IRA term in requirement language of CIP-005 R2 Parts 2.4 & 2.5.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	

Answer	No
Document Name	
Comment	
CIP-005 is not currently applicable to EACMS and PACS, along with items such as Electronic Security Perimeters, Electronic Access Points, and Interactive Remote Access. The proposed changes to CIP-005 R2.4 and R2.5 bring Interactive Remote Access applicability to EACMS / PACS. There should be clarity and differentiation between Interactive Remote Access for BES Cyber Systems / Protected Cyber Assets and vendor remote access for EACMS / PACS. Interactive Remote Access has additional controls, such as multi-factor authentication. The proposed changes can cause confusion on the applicability of Interactive Remote Access and other CIP-005 controls to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?	

Another issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I'm not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern DOES NOT agree with the addition of PACS as it has been proposed in these draft Standards as it does not align with the requirement from FERC Order 850. The SDTs has now inadvertently brought into scope corporate systems and applications that do not meet the defined terms of an Applicable System. Since PACS are not required to be in an ESP, and remote access to them is not required to traverse through an Intermediate System, then there is no existing outer boundary used for remote access to PACS assets that is in-scope. FERC has not ordered adding PACS requirements to exactly the same requirements that apply to BCS as part of this Supply Chain initiative by merely changing the Applicable Systems column. There could be less restrictive requirements or new requirements based on	

risk that could apply to PACS. We agree with the FERC Order and the NERC Study that there should be additional requirements for those PACS assets that perform "access control" functions and not merely monitoring and logging functions. Given the absence of an attempt to modify the NERC defined term for PACS to clarify the difference between PACS and PAMS, we do not agree with the addition of PACS at this time as the current definition of PACS assets to which these new requirements would apply is above and beyond the scope addressed in the FERC Order and the NERC Final Report. For these reasons, keeping requirements applicable to PACS in CIP-010 and CIP-013 addresses the FERC Order and NERC Study, however Southern believes the SDT should remove PACS from CIP-005 R2.4 and R2.5 until such time that the PACS definition can be modified and new definitions of applicable systems be added to properly scope these requirements.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging", however, this change could introduce the requirement of maintaining "lists" of PACS and what functions they provide.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	

Dislikes 0	

Response

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging", however, this change could introduce the requirement of maintaining "lists" of PACS and what functions they provide.

The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5 CIP-010-3: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4 Requirement R3 Parts 3.1 and 3.4, CIP-011-2: Requirement R1 Parts 1.1 and 1.2, Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we agree with the addition of PACS to CIP-005, CIP-010 and CIP-013, we suggest that the SDT consider creating a new requirement, CIP-005-7 R3, and move Part 2.4 and Part 2.5 to this new requirement. We believe that this will help to alleviate any confusion that may exist surrounding PACS and Intermediate Systems.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

CHPD believes that the PACS should not be added per the following discussion.

The Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommended that PCAs be excluded from CIP-013-2 because 1) the risk is difficult to quantify and 2) there is not a direct 15-minute impact related to the PCA itself. The PCAs were excluded from CIP-010 and CIP-013, but included a recommendation to address them as a best practice.

PCAs, like PACS, have no direct 15-minute BES impact. PACS, unlike PCAs, do not reside within an ESP and have no network access to the BCS or related ESP. Therefore; if PCAs are not included, it seems logical for PACS to be treated in the same manner.

The NERC Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) reasoned that PCA could be excluded from CIP-010 and CIP-013 due to the following:

1. *"The potential risk can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards and others which can be addressed in policies and procedures. For example, implementing access control lists, intrusion prevention systems, and malicious software prevention tools can be used to limit the risk posed by PCAs possibly impacting interconnected BES Cyber Systems" (p. 21).*

2. *The recommendation was to not include PCAs as "other controls deployed on the BES Cyber Systems under the CIP-007 and CIP-010 standards would protect the actual assets that could have a 15-minute impact if rendered unavailable, degraded, or misused" (p. 22).*

In conclusion, CHPD agrees with the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019) recommendation to exclude PCAs in favor of a best practice approach and adequate cyber security controls. CHPD recommends that this same reasoning be extended to PACS due to the lower potential risk to the BES.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT discussed this inclusion extensively and ultimately decided to include PACS. A review of the NERC Supply Chain Report also provides rationale for the inclusion of PACs. Specifically, the report details the following on page 24: "A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios application to compromised PACS components (such as those described above) include, but are not limited to, the following: A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements cold allow external threat actors to obtain undetected physical access to Control Centers and other Faculties that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems."	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC's conclusion in Chapter 3 of the Supply Chain Risks report that "*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*" because the conclusion is inconsistent with the current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.	

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined "[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System****. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.*" Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify cyber assets that "…. control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers," such cyber assets are appropriately classified as PACS. Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT's acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot

directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.

Likes 0	
Dislikes 0	

Response

The SDT appreciates the thorough nature of this comment and evaluated the points raised. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber

Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

The commenter seems to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

In regard to the attempt to draw a parallel between the BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to

entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
It's not clear what risk this is mitigating. Critical sites have additional protections (security guards) that are in place and will continue to provide visibility where needed in the event someone obtains unauthorized remote access to PACS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT discussed this inclusion extensively and ultimately decided to include PACS. A review of the NERC Supply Chain Report also provides rationale for the inclusion of PACs. Specifically, the report details the following on page 24: "A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios application to compromised PACS components (such as those described above) include, but are not limited to, the following: A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements cold allow external threat actors to obtain undetected physical access to Control Centers and other Faculties that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems."	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment	
Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We agree conceptually on the intent but wonder if there is a real benefits on the overall electric reliability.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No

Document Name	
Comment	

1. The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. This leads to confusion when identifying and developing procedures for cyber assets in or out of scope, when determining compliance to the standard, and at audits or when processing risk, cause, corrective and enforcement actions.

Recommend either removing the references in all revisions or revise the SAR to include a separate class of Cyber Systems which perform either the preventive control (IPS, Firewalls) or detective control functions (IDS, logging and alerting)

2. The “Applicable Systems” language does not distinguish between medium EACMS and PACS with ERC, however ERC is a consideration when classifying systems in the Parts.

Recommend initiating a revision to the Applicable Systems and Parts to address only a) EACMS and PACS with ERC as follows:

"Physical Access Control Systems (PACS) with External Routable Connectivity – Applies to each Physical Access Control System with ERC and associated with a referenced high impact or medium impact BES Cyber System"

"Electronic Access Control or Monitoring Systems (EACMS) with External Routable Connectivity – Applies to each Electronic Access Control or Monitoring System with ERC and associated with a referenced high or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems."

3. CIP-010-4 – “Applicable Systems” – PACS (pp5-6) includes for PACS “except as provided in Requirement R1, Part 1.6.” This is confusing and potentially adds Cyber Systems into scope which are not in scope

Recommend updating the Applicable Systems definitions to match the Parts where ERC is or is not required.

4. CIP-010-4 Part R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 0	

Dislikes 0	

Response

The SDT thanks you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS or PACS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS or PACS is outside the SAR for this SDT due to EACMS and PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging" or "EACMS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and PACS and what functions they provide.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 of CIP-010-4 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE agrees conceptually with including PACS but needs to assess the risk and implementation. However, we expect a lower return on investment on PACS.

There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure.

Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?

We agree with the proposed changes. *We do see one issue with the change to the applicability of PACS on page 6 of the redlined standard document for CIP-010-4. We question whether the exception should be added or maybe it needs to also include part 1.1. I'm not sure it makes sense to include additional devices in part 1.6 that are not included in 1.1 given that 1.6 must be followed only when there is a change to the baseline defined in 1.1*

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	

Comment
Alliant Energy does not oppose the addition of PACS, but agrees with the NSRF that consideration and clarity is needed around Medium Impact BES Cyber Systems with and without External Routable Connectivity.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within: CIP-007-6: Requirement R2 Parts 2.1, 2.2, and 2.3, Requirement R3 Parts 3.1, 3.2, and 3.3, Requirement R4 Part 4.1, Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5 CIP-009-6: Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E agrees with the addition of PACS but does not agree with the use of PACS as currently defined in the "Applicable System Columns in Tables" section of the Standard. Including PACS which only provide monitoring or alerting capabilities in the modifications extends what was indicated in the NERC supply chain study recommendation which indicated only "access control" capabilities. PG&E believes the risk of PACS which "only" provides monitoring and alerting capabilities is not the same as those which provide "access control" capabilities and should be excluded from the Standard. PG&E does indicate if a PACS provides access control while at the same time monitoring and/or alerting capabilities it should be covered by the Standard.

PG&E recommends the definition in the "Applicable System Columns in Tables" section be altered to indicate only those PACS which provide "access control" and that PACS that only provide monitoring and alerting be excluded. A Technical Rationale document could be created to clearly indicate what type of PACS would be covered with examples to help clarify any confusion. A potential benefit in making

the “Applicable Systems Column in Table” indicate PACS with only “access control” is to the Project 2016-02 SDT working on the separation of PACS into Cyber Assets for “access control” (PACS) and monitoring/alerting (PAMS). A clear indication of “access control” in the Project 2019-03 modifications could make it easier for the Project 2016.-02 SDT to make conforming changes to CIP-005, CIP-010, and CIP-013 once they are ready to complete the work on the PACS separation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as “PACS, excluding those that provide only alerting and logging”, however, this change could introduce the requirement of maintaining “lists” of PACS and what functions they provide.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We agree conceptually with including PACS but need to assess the risk and implementation. However, we expect a lower return on investment on PACS. There should be some awareness message on the change for CIP-010-4 R1.6 on third party or shared infrastructure. Was it intentional to not capitalize electronic access point in CIP-005 R2.5 bullet three of the measures?	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting. Those with shared infrastructure (co-located or jointly owned BES facilities) need to review and reevaluate their agreements based on new or revised requirements. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2.	

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC and GTC do not agree with or support the addition of PACS to the applicable systems for the supply chain reliability standards. In particular, GSOC and GTC are concerned regarding NERC's conclusion in Chapter 3 of the Supply Chain Risks report that "*…if compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES*" because the conclusion is inconsistent with the current classification of PACS components in a category distinct from BES Cyber Assets, and because a compromise of a PACS would not have a real-time impact on the BES without a secondary action.

In accordance with the typical implementation of reliability standard CIP-002-5.1a and pursuant to the NERC-approved definition, if a cyber asset has or could have a direct impact on the reliability of the BES, it ***must be characterized*** as a BES Cyber Asset. A BES Cyber Asset is defined "[a] *Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed,* ***would affect the reliable operation of the Bulk Electric System****. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.*" Importantly, cyber assets that are classified as PACS are classified as such because they perform unique functions required by the CIP reliability standards, including, but not limited to CIP-006, CIP-004, etc. Hence, where responsible entities identify cyber assets that "…. control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers," such cyber assets are appropriately classified as PACS. Thus, it is difficult to reach the same conclusion as NERC and the SDT, e.g., that a compromise, misuse, or rendering unavailability to PACS components would directly affect the reliable operation of the BES.

More importantly, though, these definitions form the foundation of cyber asset classification and the overall industry interpretation of how its cyber assets should be classified. The assertion by NERC that PACS directly impact the reliability of the BES and the SDT's acceptance of this to justify their inclusion in the applicability for the supply chain reliability standards effectively upends nearly a decade

of Commission, ERO, and industry precedent regarding what constitutes a BES Cyber Asset and what constitutes supporting cyber assets such as PACS.

GSOC and GTC acknowledge that the compromise, misuse, or rendering unavailable of PACS could be an initiating action for a secondary action of compromise, misuse, or rendering unavailable of a BES Cyber Asset or other cyber asset when determining adverse impact to the reliability of the BES. However, the singular, isolated cyber compromise to PACS without other secondary action does not and would not have real-time impacts on the reliability of the BES. More specifically, without a concurrent or subsequent physical compromise, the compromise, misuse, or rendering unavailable of a PACS alone cannot have a direct impact on the reliability of the BES. A second order of physical presence by way of entry into the Physical Security Perimeter must occur to impact reliability.

The inclusion of secondary actions when determining direct impacts is atypical generally and is also inapposite to the risk-based nature of the CIP reliability standards, the BES Cyber Asset definition, and the significance of asset redundancy as a risk mitigating strategy. The need for a secondary action (physical security compromise) and – potentially- a tertiary action (e.g., the compromise, misuse, or rendering unavailable of a BES Cyber Asset or BES asset equipment) clearly demonstrates that adverse action to PACS alone cannot directly impact the reliability of the BES. Given this reality, PACS would not and should not (in the CIP reliability standards risk based framework) require the same protections as those cyber assets that could directly impact the reliability of the BES.

NERC correctly refers to various Reliability Standards that mitigate security risks relating to PACS. These include CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GSOC and GTC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see response at the beginning of Q2, which is also included in Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	
Comment	

We agree with the addition of PACS (and EACMS) to CIP-005-7 and CIP-013-2, but a close examination of the currently approved definition(s) of PACS (and EACMS) prevents them from being added to Medium Impact BES Cyber Systems in CIP-010-4 Requirement R1, Part 1.6 as proposed.

PACS are currently defined as:

“Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.”

PACS are tied to PSPs. PSPs only exist with respect to Medium Impact BES Cyber Systems for those with ERC per CIP-006-6 Requirement R1, Part 1.2. Medium Impact BES Cyber Systems without External Routable Connectivity are only required to define operational or procedural controls to restrict physical access; a PACS is not required.

We recommend, for clarity and consistency among CIP standards:

1.) Insert:

“Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and

2. PACS”

Between High Impact and Medium Impact Applicable Systems in CIP-010-4 Requirement R1, Part 1.6.

2.) Delete “except as provided in Requirement R1, Part 1.6” from the PACS description in the Background on p. 6.

Although the PACS applicability language does not directly affect CIP-005-7, we recommend that the new inclusion of PACS applicability in the Background on p. 6 include "with External Routable Connectivity" to be consistent with most of the standards. CIP-006-6 and CIP-007-6 should likewise be corrected during the next revision.

CIP-006-6 and CIP-007-6 language:

"Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System."

CIP-004-6, CIP-009-6, CIP-010-3 and CIP-011-2 language:

"Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity."

Also, in keeping with the same principle, for CIP-013-2, we suggest changing Requirement R1, "for high and medium impact BES Cyber Systems and their associated EACMS and PACS," to "for high and medium impact BES Cyber Systems, and EACMS and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity."

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment.

At this time there is no separation of access control vs. monitoring within the approved definition of PACS and the SDT must use approved definitions. Additionally, a change to the definition of PACS is outside the SAR for this SDT due to PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging", however, this change could introduce the requirement of maintaining "lists" of PACS and what functions they provide.

The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered

Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards. The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We agree to add PACS to the applicable systems but disagree with the language regarding PACS in CIP-013-2 R1 and CIP-010-4 Section 6 Background since it would bring PACS associated with BCS w/o ERC into scope. Currently It has been commonly understood that only PACS associated with BCS with ERC is applicable to the CIP standards based on CIP-006 R1.1 requirement in which PACS is not required for medium impact BCS without ERC. We suggest making the following changes: For CIP-013-2 R1, Part 1.1 and Part 1.2, change “high and medium impact BES Cyber Systems and their associated EACMS and PACS” to “high and medium impact BES Cyber Systems and their associated EACMS, and PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.” For CIP-010-4, remove the wording “except as provided in Requirement R1, Part 1.6.” from Section 6 Background.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees with the commenters’ statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used	

this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2,

As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Adding PACs is not necessary. The standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Adding PACS is not necessary. The standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
sean erickson - Western Area Power Administration - 1	

Answer	No
Document Name	
Comment	

The **NERC Cyber Security Supply Chain Risks** white paper recommendations excludes a) EACMS which provide monitoring and logging and b) PACS which perform alarming and logging services. The applicability and definitions in the revisions do not distinguish between preventive (firewalls) and detective (monitoring/alarming/logging) EACMS and PACS. In addition, the Applicable Systems and language does not distinguish between EACMS and PACS with ERC. Recommend revising Definitions, Applicable Systems and Parts to address only EAMCS and PACS with ERC and which perform preventive security services.

CIP-010-4 – Applicable Systems – PACS (pp5-6): current term of a PACS "except as provided in Requirement R1, Part 1.6." adds Cyber Systems into scope which are not in scope. It is not clear and confusing.

CIP-010-4 R1.6 – does not distinguish BCS with ERC from BCS without – in context, adds Cyber Systems to this requirement which are not in scope for the FERC Order 850 or NERC Cyber Security Supply Chain Risks white paper

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS or PACS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS or PACS is outside the SAR for this SDT due to EACMS and PACS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "PACS, excluding those that provide only alerting and logging" or "EACMS, excluding those that provide only monitoring and logging":, however, this change could introduce the requirement of maintaining "lists" of EAMCS and PACS and what functions they provide.

The SDT reviewed the formerly proposed exception within the applicability of PACS on page 6 and determined it was unnecessary. Please see the redline draft of CIP-010-4.

The SDT agrees with the commenters' statements that EACMS and PACS are a concept only applicable to BES Cyber Systems (BCS) with External Routable Connectivity (ERC) and asserts that the existing proposed applicability carries that meaning. By definition, Registered Entities with medium impact BCS without ERC would have a null list of associated EACMS and PACS rendering the requirement for associated EACMS and PACS inapplicable and unimpactful. The 2019-03 SDT, and former SDTs, have used this construct for requirements that apply to both medium impact BES Cyber Systems with and without ERC, relying on the qualifiers in the "Background" section of the Standard to further clarify EACMS and PACS are only in scope where ERC is present, in addition to the definitions that already support this same intention. Additionally, this is not a new condition; in fact, it is a commonly used and pervasive construct in the existing standards that presents itself in the exact same form within:

CIP-007-6:

Requirement R2 Parts 2.1, 2.2, and 2.3,

Requirement R3 Parts 3.1, 3.2, and 3.3,

Requirement R4 Part 4.1,

Requirement R5 Parts 5.1, 5.2, 5.4, and 5.5

CIP-009-6:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.5

CIP-010-3:

Requirement R1 Parts 1.1, 1.2, 1.3, and 1.4

Requirement R3 Parts 3.1 and 3.4,

CIP-011-2:

Requirement R1 Parts 1.1 and 1.2,

Requirement R2 Parts 2.1 and 2.2, As a result, the SDT has retained the applicability as proposed to keep it consistent with not only the other six Requirement Parts within CIP-010, but also the other 19 aforementioned Requirement Parts within three other currently enforceable versions existing CIP Standards.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Adding PACS is not necessary. The Standards as they are right now are just fine.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT was tasked with execution of FERC order 850 and has strived to complete that task.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Tampa Elecric does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	

Answer	Yes
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC requests clarification. Was it the SDT's intent not to capitalize "electronic access point" and "intermediate system" under CIP-005-7, requirement R2, part 2.5, bullet three under Measures? NYISO doesn't understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has fixed the capitalization issue in CIP-005-7 R2.5 which is now R3.2. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity around remote access requirements.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and does not oppose the addition of PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees with adding PACS to the Supply Chain Standards as currently described above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Cynthia Lee - Exelon - 5	
Answer	

Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

3. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL's. A violation of failing to have a method for determining OR disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining AND disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. They should be low, or better yet not a violation at all.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
They should be low, or better yet not a violation at all.	

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	

Comment
They should be low, or better yet not a violation at all.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	

Comment

Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Since PACS are listed in the requirement language, there must be an associated reference to them in the VSL so they cannot be removed completely. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed. 1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established. We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis: "… where permitted and not otherwise blocked or unable to be established…" R2.5 can then be changed to add "according to R2.4 above" before the parenthesis.	

2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions: Expand EACMS to "EACMS that provide electronic access control (excluding monitoring and logging)," or equivalent language. Expand PACS to "PACS that provide physical access control (excluding alerting and logging)"	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. In response to EACMS and PACS definitions, please see response to MRO from questions 1 and 2 above.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to GSOC and GTC from questions 1 and 2 above.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
The wording is awkward and should be clarified to explain that failing to have one of the two methods required (determining OR disabling) is a moderate VSL while failure to have any of the required methods (lacking BOTH a means to determine and lacking a means to disable) is a high VSL.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT modified the VSL language to make this distinction clearer. Please note, the previous CIP-005-7 R2.4 and R2.5 have now been moved to R3.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the modified VSLs, but agrees with the NSRF that the language should be clarified for the scenario where a Responsible Entity does not permit vendor remote access sessions for some or all vendors. Alliant Energy also supports the NSRF's comments to update the applicability section to include only EACMS that provide electronic access control (excluding monitoring and logging) and PACS that provide physical access control (excluding alerting and logging).	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. In reference to EACMS and PACS definitions, please see responses to MRO in questions 1 and 2 above.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE disagrees with adding EACMS and PACS to CIP-005. CIP-005 was intended for access to High and PCA systems. In fact, EACMs are derived from the CIP-005 requirements. The CIP standards and requirements are structured to address security concerns based on the criticality and risk to the BES. EACMS and PACS do not incur the same security concerns and do not have the same criticality or risk to the BES; therefore, EACMS and especially PACS should not be treated the same as High or Medium Impact systems that have a	

direct correlation to the reliability of the BES. Additionally, the co-mingled definition of “access control and monitoring” inherently elevates systems with monitoring only capability to a high-water mark, adding the need to incorporate burdensome and costly controls to extremely low risk systems for little benefit. In support of the lower impact and risk, both VSLs should be listed as minimal to moderate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2. In reference to EACMS and PACS, please see response from question 1.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Due to the low risks Vendor remote access to PACS have to the operation of the BES, we feel the VSLs should be the lowest possible. The protections and requirements already afforded to Vendor remote access to PACS: access control, PRAs, training, etc., already reduce the risks PACS pose to the BES. The new requirements are a best practice, and do not have a high enough risk level to warrant a Medium or High VSL.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Agree with Duke Energy's comment. "Since PACS poses a lower risk to the BES, Duke Energy suggests that the VSLs should be lowered and should be no higher than Low or Moderate."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT maintains that the VSLs of moderate for failing to have a method for determining OR disabling for PACS, and high for determining AND disabling are appropriate. For more information see the Technical Rationale for CIP-005-7, CIP-010-4 and CIP-013-2.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Although the CAISO acknowledges that PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from	

audit experiences including findings and areas of concerns identified by the auditors. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
If PACS was added, which I disagree with, the modified VSLs can help at the time of enforcement, but don't help during implementation. VSLs are not evaluated when determining how to implement CIP requirements and VSLs do not influence the level of effort applied to protect the BES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

We agree with the modified VSLs, but believe there are underlying problems with CIP-005-7 R2.4 and R2.5 as currently proposed.

1.) The requirements assume vendor remote access sessions and impose additional monitoring requirements upon all Responsible Entities regardless of whether or not a Responsible Entity permits vendor remote access sessions. There is no need for this ongoing requirement if an entity decides not to permit vendor remote access sessions and has ensured that such sessions are either blocked or not able to be established.

We recommend R2.4 be changed to add the following, or equivalent language, before the parenthesis:

"… where permitted and not otherwise blocked or unable to be established…"

R2.5 can then be changed to add "according to R2.4 above" before the parenthesis.

2.) Per the Background Information provided at the beginning of this comment form, we propose the following change to the Applicable Systems for R2.4 and R2.5 as a means of meeting the NERC supply chain report recommendations to include (i) EACMS that provide electronic access control (excluding monitoring and logging) (p. 7), and (ii) PACS that provide physical access control, excluding alerting and logging (p. 12) while retaining current definitions:

Expand EACMS to "EACMS that provide electronic access control (excluding monitoring and logging)," or equivalent language.

Expand PACS to "PACS that provide physical access control (excluding alerting and logging)"

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. Please see responses to PACS and EACMS definitions in questions 1 and 2.

Greg Davis - Georgia Transmission Corporation - 1

Answer	No

Document Name	
Comment	
While GSOC and GTC agree that the VSLs and VRFs associated with the addition of PACS should be lower, as discussed above, GSOC and GTC disagree with the addition of PACS to these requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to GSCO and GTC in questions 1 and 2 above.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO in questions 1 and 2 above.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	

Based on response under question #2 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 2 above.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO in questions 1 and 2 above.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No Comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the indicated VSL assignments for PACS.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Xcel Energy supports EEI comments and does not oppose the changes to VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
NYISO doesn't understand the applicability for controls for remote access regarding PACS devices as implied within CIP-005 remote access requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT thanks you for your comment and have moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity around vendor remote access.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	

Answer	Yes
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to questions 1 and 2 above.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the modifications made to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the modifications to the VSL's. However, see our comments in questions 1 and 2 with regard to the addition of EACMS and PACS assets to the scope of these new requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see response to questions 1 and 2 above.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Tampa Elecric supports the modifications made to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

SDT General Response to Question 4

Thank you for your comment, there have been significant discussions referring to the comments proposed by EEI and their recommendation. It has been proposed that the SDT expand the implementation time to 18 months based on the following criteria:

- EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts.
- The large number of vendors and their contracts that are currently in place may need to be modified and renegotiated to cover any new existing equipment and systems that would need to be put in place.
- Vendors are possibly placed in several regions and jurisdictions and would take more time to consolidate the same policies and procedures across the entity.

In addition, outside of the EEI recommendations, other entities have expressed the consideration of budget cycles due to technological upgrades needed for the implementation along with the budgeting and planning efforts within most entities occur annually with the planning and finalization occurring a year in advance. Those technology upgrades would include but not limited to:

- Implementing a Governance, Risk, and Compliance (GRC) solution if not already deployed within their organization, i.e. Archer, Appian, etc.
- A Third Part Risk Management (TPRM) solution in concert with the entities' Supply Chain Management, i.e., Archer, Fortress Information Security, etc.

An 18-month implementation plan would allow organizations to address any change management, possible contract revisions, vendor additions, budget cycles, and policy modifications to be put in place in a timely manner.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No

Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	

We would prefer an 18 month implementation to better accommodate a budget cycle	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Tampa Elecric supports EEI recommendation that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	

Comment	
Eversource suggests an 18-month implementation plan due to current experience with adding vendors to the initial Supply Chain project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
We recommend a longer implementation period than the proposed 12 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern recommends that the SDT expand the proposed time for implementation plan to 18 months and suggests for the SDT to consider budget cycles for possible technological upgrades needed before implementation. In this case, 18 months would be a fair alternate time frame. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No

Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors, entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, the additional time to implement the standard is necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	No
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 4	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	No
Document Name	
Comment	
The IRC SRC recommends an 18- or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they will need to develop and implement a different process for EACMS and PACS systems. Therefore, the IRC SRC requests the SDT allow additional time. Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 4.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports EEI comments on this question and believes that an 18 month implementation period would be more appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are	

embedded. Introduction of electronic access control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity's existing program. Therefore, we strongly disagree with the assertion that the changes are administrative. Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes. For these reasons, GSOC and GTC recommend a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	No
Document Name	
Comment	
MPC does not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature. Budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes. For these reasons, MPC recommends an 18 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
Because EACMS and PACS may be located outside of any Electronic Security Perimeter (Intermediate Systems MUST be outside any ESP), N&ST believes entities *could* find it necessary to define and implement controls for CIP-005 R2.4 and R2.5 for EACMS and PACS that are entirely different than the ones they have implemented for BES Cyber Systems and PCAs. Therefore, N&ST believes the implementation plan duration should be 18 months, not 12 months.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24 month implementation plan after the applicable governmental entity's order approving the standard to allow entities flexibility to determine the appropriate implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The proposed implementation timeline may not allow enough time for industry to properly gauge the effects of the preceding version of standards Subject to Enforcement. Based on the outcomes of the yet to become effective versions of the Standards, additional budget and time could be needed to implement the proposed updates. SRP would like to recommend an implementation timeline of 15 to 18 calendar months, starting in the next calendar quarter of the approval of CIP-005-7, CIP-010-4, and CIP-013-2.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
The IRC SRC recommends an 18 or 24-month Implementation Plan to allow sufficient lead time for an entity to incorporate changes into their programs as time will be needed to justify costs and obtain budgets as well as developing approaches to accommodate the expansion of assets included in scope. Depending upon how an entity implemented their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they will need to develop and implement a different process for EACMS and PACS systems, so the IRC SRC requests the SDT allow additional time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Considering the scope of changes introduced by SDT, we recommend an 18 or 24 month implementation plan.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Jamie Prater - Entergy - 5	
Answer	No
Document Name	
Comment	
Entergy proposes an 18 month implementation plan as was approved via Project 2016-03 for these standards. While the requirement language does not change, the inclusion of systems that were not originally included in the Project 2016-03 scope should allow for the same timeline of implementation as entities must again evaluate compliance strategies for new sets of hardware and/or software that may not be compatible with the entity's expected processes for BCA and PCA assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Agree with Duke Energy's comment. "Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve a longer time-horizon, capital budgets and planning cycles."	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
18 months minimum	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Although adding the words EACMs and PACS to the requirements seems fairly innocuous. It can in fact be a significant impact to an Entity's CIP compliance program and approach. Entities may need to evaluate, procure and implement new technologies and processes to incorporate these systems.	

Recommend a 24 month implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments recommending that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS represents a significant expansion in scope for both hardware and software covered under existing contracts. Entities have a large volume of vendors each of which has different contracts in place. Thus, for each of the vendors,	

entities will need to modify existing policies and processes and negotiate modified contracts with the many existing vendors to cover new equipment and systems. In addition, the new requirements will require conducting negotiations with new vendors.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
From participation NERC and industry discussions, it appears that the basis for a 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high and medium impact BES Cyber Systems. This supposition would make it appear that it is a straightforward expansion of existing Supply Chain programs to EACMS and PACS. This is not true in all cases. Notably, the high (control center) and medium (ex. substation) impact environments are very different. CEHE suggest that 12 months is not sufficient and would like to propose a 24 month implementation plan instead.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	

Comment	
FE recommends that the SDT expand the proposed time for implementation plan to 18 months. The addition of EACMS and PACS will result in a significant expansion in scope for both hardware and software covered under existing contracts. Entities will need to modify existing policies and processes and negotiate modified contracts with existing vendors to cover new equipment and systems. In addition, these new requirements will require conducting negotiations with new vendors. In all cases, such efforts are time consuming, especially for entities that have many vendors in multiple jurisdictions. Therefore, we feel additional time will be required to implement the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
NPCC recommends an 18 or 24 month Implementation Plan due to entity budget cycles and significant increases in scope for the entity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
The addition of system-to-system access will take defining and further investigation; BPA believes this is a larger change than we can accomplish in 12 months. Also, Projects 2016-02 and 2019-03 definitions and implementation dates must be reconciled.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC and GTC do not agree that the addition of EACMS to the Supply Chain Standards is only administrative in nature.

The current applicability consists only of High and Medium Impact BES Cyber Systems and associated Protected Cyber Assets. The nature and makeup of systems that perform the function of electronic access control are materially different than those that perform functions of BES Cyber Systems. For instance, consider a substation environment. One can reasonably envision a program that consists entirely of protective relays, remote terminal units, data concentrator, carrier radios, etc. Note that the nature of all of these systems are embedded. Introduction of electronic access control systems introduces entirely new classes of infrastructure, including software that may not even be considered in an entity's existing program. Therefore, we strongly disagree with the assertion that the changes are administrative.

Furthermore, budgeting and planning efforts within most electric utility organizations occur at least annually with budget and/or project planning and finalization for each year occurring in advance of the implementing year. Often, major system replacements and upgrades are planned more than a year in advance of the anticipated implementing year. Further, responsible entities with contract/procurement management systems that are facilitating their CIP-013 compliance may have technical/programming needs to modify these corporate procurement systems to include EACMS for compliance reporting purposes.

For these reasons, GSOC and GTC recommend a 24 month implementation plan.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment. Please see the SDT response at the beginning of question 4.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO

Answer	No
Document Name	

Comment

The NSRF recommends an overall 18-month implementation plan. The SDT is already changing yet to be effective Standards whereby applicable entities will need to prove compliance then add additional compliance attributes (PACS and EACMS). There may be new

entities who will need to start a new portion of their compliance program to satisfy these new attributes. Recommend an 18-month implementation plan.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends a 24-month implementation plan as technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve a longer time-horizon, capital budgets and planning cycles.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Should be 48 months or longer.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Should be 48-months or longer.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
We propose an 18 month implementation plan in order to address change management: understand the impact to existing programs, processes and documentation, revise existing documentation, develop and implement changes and test changes for integrity.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NO. Should be 48-months, or longer.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC reccommends the SDT modify the current implementation plan to allow entities 18 months to fully implement the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	

Answer	No
Document Name	
Comment	
18 month is more reasonable since 12 month will be hard for entities that have many vendors to meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
Some smaller entities may not have the resouces or time to allocate with only a one year implementation. Typically our budgets are very tight and are set one year in advance, in October. A longer implementaiton time assures we have resouces that can be allocated through the annual budget process.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's recommendation that the SDT expand the proposed time for the implementation plan to 18 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the proposed 12-month implementation plan. PG&E believes the Cyber Assets being brought into scope for this modification should be able to follow the same plans and processes being developed for the BES Cyber Systems (BCS) under CIP-013-1. PG&E does not anticipate significant changes to the plans or processes would need to be done exempt for an indicating that EACMS and PACS must be covered, and believes the education of personnel handling the procurement and implementation of the Part 1.2 controls for EACMS and PACS should be able to be done within the 12-month interval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Cynthia Lee - Exelon - 5	

Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 4.	

5. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

A scope change of applicable CIP system always cause additional compliance cost. We don't know whether the current change is cost-effective or not.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
One member entity estimated the following costs and provides a recommendation: Depending on the entity, the costs associated with the proposed changes may range between an annualized cost of $80K (80 to 100 hours per person) and $500K per entity. This does not include capital expenditures for technologies which manage vendor access, which may exceed $5M per entity. This is based on the need to: a. Develop, update and implement procedures and training for multiple departments and their personnel. b. Perform updates to existing categorization processes to ensure the identification and controls exist to meet and exceed the requirements in the revisions. c. Identify existing or implement new technologies to manage supplier or vendor remote access solutions. This includes efforts in integration and changes to systems, contracts, processes and internal compliance program metrics.	

Recommend utilizing existing CIP program processes to meet the requirements. For example, CIP-013 R1.5 requires software integrity in the supply chain. CIP-010 R1.6 requires software integrity. CIP-007 R2 also requires integrity in software security patches. Aligning those standards into a single meaningful standard could improve cost effectiveness.	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
BPA supports WAPA's comment as follows: "The costs associated with ensuring supply chain and CIP-010 R1.6 and CIP-013 R1.2.5 - integrity of software in the supply chain, as well as the requirement to have multi-departmental personnel, updates to existing documentation, new documentation, changes to systems and contract changes will cost industry and ratepayers many thousands of dollars in personnel, systems and process work."	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E cannot agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1 has not been completed and a full understanding of the current costs is not known. PG&E would have preferred to answer this question as "Unknown", but the option was not available.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
NERC should perform an impact analysis as part of the SAR process. Every change impacts existing documentation and process stacks.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Although the CAISO acknowledges that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on wait with extending the program to EACMS and PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least a two years to allow for the processes and controls to mature, to obtain any key learnings from implementing these protections and from audit experiences including findings and areas of concerns identified by the auditors to ensure they are implemented in the most cost-effective manner. At that time the CAISO also proposes NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, however, FERC order 850 has an implicit deadline of December 1, 2020.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The FERC order states this is only an "increased paperwork burden" which I disagree with. Where does this include the actual ongoing monitoring of activity and maintaining an adequate level of training personnel across multiple parts of the power systems that know how to respond?	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Prior to proposing additional modifications, Reclamation recommends each SDT take additional time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities economic relief by allowing technical compliance with current standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

While GSOC and GTC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	

Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	

Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the FERC directives can be executed in a cost-effective manner. There will be an undue cost and burden initially to conduct business another way by adding EACMS and PACS to CIP-005 R2.4 and R2.5. Other costs will include providing new technology if not already present to track, store, and recall the data addressing the assessments provided by CIP vendors. One suggestion would be to allow the additional time suggested in Question 4 to consider those budget cycles for any possible technology upgrades.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Re-use of existing terms is easier and more cost effective than introducing new terms and/or requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Reinecke - Seminole Electric Cooperative, Inc. - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.	

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities!

Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes.

NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions.

And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.

Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.

Scott Tomashefsky - Northern California Power Agency - 4

Answer	
Document Name	

Comment

NERC needs to include the real costs of all new regulations they are imposing not the low ball figures they have provided in the past.

The costs impacts on entities due to the constant changing of Standards and having entities change documents we just changed needs to be included. Lost productivity time cost of getting modified documents and budgets approved and implemented (once again due to NERC program changes) by our governing boards cost of lost opportunities! Also they need to include costs for specific new FTEs (SMEs, persons to insure project controls in place, persons to quality check new controls). Plus they need to include cost of changing/Updating existing plans and policies, cost to send out new RFPs to Vendors, cost for additional/updated Vendor reviews per another set a CIP standards changes. NERC is proposing these new changes when the Supply Chain Standard has not even taken effect yet nor have prior approved CIP-005 and 10 July 1, 2020 effectives versions. And now they are proposing changes to these standards, again. They are working on more proposed changes, see project 2016-02. In my view all these multiple changes and proposals are unnecessary and costly to entities; let only confusing to use, our governing boards, and have little, if any, real reliability value.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
No Comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your response.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy takes no position on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 5.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your response.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
Tampa Electric takes no position as to the cost effectiveness of the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

6. Provide any additional comments for the standard drafting team to consider, if desired.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI for question 6 below.	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
The proposed changes to include EACMS and PAC to the CIP-010-4 requirements seem reasonable, but will add to workload.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	

Document Name	
Comment	
Tampa Electric supports the following EEI comments: In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states "[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.") With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access. In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you've entered the "hall of mirrors"). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5. EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT	

considered adding qualifying language to the standard such as “EACMS, excluding those that provide only monitoring and logging”, however, this change could introduce the requirement of maintaining “lists” of EACMS and what functions they provide. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE seeks clarification as to why PACS and EACMS were not added as applicable systems for Parts 2.1-2.3. In the scenario where a vendor is utilizing Interactive Remote Access (IRA) to a BCA or PCA, Parts 2.1-2.5 would be applicable. However, if the vendor is utilizing IRA to a PACS or EACMS, Parts 2.1-2.3 would not be applicable. This would mean no Intermediate System, no encryption, or multi-factor authentication is required. Texas RE recommends PACS and EACMS should be added.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes this is outside the scope of our SAR.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC	
Answer	
Document Name	
Comment	

During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and NPCC request written clarification if mitigation will be required in CIP-013-2 R1. There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months …." However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months …."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2. The SDT has corrected the error in CIP-010-4 R3 moderate VSL.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern's comments were detailed in Questions 1-5.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses in questions 1-5.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MidAmerican agrees with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
In this draft, the SDT has chosen to include all EACMS while the Commission provided the SDT with enough latitude to include only those EACMS that represent a known risk to the BES. (see Order 850, P51 where the Commission states "[We] leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risks. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems.") With this in mind, we encourage the SDT to reevaluate its approach and develop more targeted modification that only address the known risks associated with EACMS that perform the function of controlling electronic access.	

In addition to the concerns stated above, EEI also disagrees with the change made to proposed Reliability Standard CIP-005-7, Requirement 2, Subpart 2.5. While on the surface the change might appear to address the order, the change can be interpreted in such a way that would create an untenable dilemma. The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall). Unfortunately, this solution is unworkable because the new firewall would become a new EACMS obligating the entity to again install another firewall creating an endless loop of new obligations (i.e., you've entered the "hall of mirrors"). To resolve this issue, we recommend simply removing PACS and EACMS from the applicability section of Requirement R2, Subpart 2.5. EEI also urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes. The changes offered raise many questions on how best to develop and implement solutions that achieve effective compliance. Such guidance will help entities to better understand the proposed changes offered by the SDT.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EACMS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Great Plains Energy - Kansas City Power and Light Co., ; James McBee, Westar Energy, 1, 6, 5, 3; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., ; John Carlson, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., ; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb	
Answer	
Document Name	
Comment	
Westar Energy, an Evergy company, supports Edison Electric Institutes responses to Question 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	

1. The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs.

2. The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of CIP-013-2 requirement R1 with the *proposed* language for CIP-011-3, requirement R1, part 1.4. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks," there is no mention of mitigation (see excerpt below):

"One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)."

Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to "identify, assess and ***mitigate*** risks in cases where vendors store Responsible Entity's BES Cyber System Information."

The IRC SRC requests the SDT collaborate with the SDT for Project 2019-02 to clarify and align the intent of this proposal with respect to mitigation:

a. Modify the language under proposed under CIP-011-3, requirement R1, part 1.4 to align with CIP-013-2, requirement R1, part 1.1 ***OR***

b. Migrate all proposed vendor-related requirements under Project 2019-02: BCSI Access Management (i.e. CIP-011-3, requirement R1, part 1.4) to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.

The IRC SRC believes the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope:

"This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements."

Note: CAISO (segment 2, WECC region) also joins the IRC SRC in the comments provided in response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments on this question. In addition, upon evaluation of the addition of EACMS to CIP-005-6 R2.4 and R2.5, Xcel Energy has recognized that the requirement may limit additional controls to address the risks the requirement part is intended to address. This situation may create additional administrative burden without the consummate benefits that could be gained through policy or procedural controls. In CIP-005-6 R2.4 the Requirement states that a Responsible Entity (RE) shall "have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)". In CIP-005-6 R2.5 the requirement states that a RE shall "have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)." Both requirements assume that RE have systems that have the capability of Vendor Remote Access (VRA) and that the RE allows for VRA if capability exists. Many entities may have systems that are not capable of VRA or do not allow for VRA in their programs. Yet the requirement as written would still force a RE to implement methods to determine VRA sessions and implement methods to disable VRA sessions. Xcel Energy believes that this issue would be eliminated by adding limited language to the Requirements that reduces the scope to only those REs that allow for VRA.	

Xcel Energy proposes adding the following or similar language to achieve this goal:

CIP-005-6 R2.4:

"Where the Responsible Entity permits vendor remote access, have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)."

CIP-005-6 R2.5:

"Where the Responsible Entity permits vendor remote access, have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

Xcel Energy believes these changes can be made within the scope of the current Standard Authorization Request (SAR). In the purpose section of the SAR the Standard Drafting Team (SDT) is directed to address directives issued by FERC in Order 850 and consider NERC Staff recommendations from the NERC Staff Report. In the Cyber Security Supply Chain Risks Staff Report where they state in the Recommended Actions to Address the Risks section of CH2, P9-10 that recommended actions should "include recommendations to address EACMS risks in the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk as follows:"

· "Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, include recommendations relative to coordinated controls between the entity and applicable vendors associated with CIP-005-6 (Parts 2.4 and 2.5) for managing active vendor remote access sessions to and/or through EACMS cyber asset types".

In the process of addressing risk of VRA the SDT should recognize that a VRA risk is being addressed through policy or procedural controls, which current Requirement language does not allow for. If EACMS were included in the scope of the original Supply Chain project this ambiguity in requirement language could have been addressed at that time.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT has provided draft guidance around scenarios where a Responsible Entity does not permit vender remote access sessions in CIP-005-7 Implementation Guidance. Please see response to EEI in question 6.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon will align with EEI's comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has aligned with EEI's comment in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	

David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
There are cases where the requirements would include “BES Cyber Systems, and their associated EACMS and PACS” as Applicable Systems (such as in CIP-010-4 Part 1.6, CIP-013-2 R1, R1.1, R1.2, R1.2.5). If associated PCAs are not included, the rest of the cyber assets within an Electronic Security Perimeter are also vulnerable. For example, PCA patches may be inadvertently loaded with Trojan Horses, malicious sniffers, etc., which may affect the rest of the devices in the network – including BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PCA’s are not in scope for this SAR.	
Monika Montez - California ISO - 2 - WECC	

Answer	
Document Name	
Comment	

The IRC SRC recommends the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4 "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below in the form of a divergence in language between the two SDTs.

During discussion with a member of the SDT, the member indicated mitigation would be required for CIP-013-2 requirement R1. Currently, the language of CIP-013-2, R1, part 1.1 only requires an entity to "identify and assess cyber security risks" and not mitigate them as detailed below.

"One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)."

That said, the parallel SDT team working on Project 2019-02: BCSI Access Management has *proposed* language for CIP-011-3, requirement R1, part 1.4 that will require an entity to "identify, assess and ***mitigate*** risks" as detailed below:

"Processes to identify, assess, and ***mitigate*** risks in cases where vendors store Responsible Entity's BES Cyber System Information."

If the intent of this proposal is to require mitigation for ***all*** assets under CIP-013, requirement R1, part 1.1, the IRC SRC requests the SDT to:

- Modify the language under CIP-013-2, requirement R1, part 1.1 to mirror the language proposed under CIP-011-3, requirement R1, part 1.4 ***OR***

Migrate all proposed vendor-related requirements under Project 2019-02; i.e. CIP-011-3, requirement R1, part 1.4, to Project 2019-03: Cyber Security Supply Chain Risks so that they can be addressed collectively under CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
To prevent possible confusion we suggest that all modifications proposed for CIP-005 and CIP-010 should be documented in one CIP standard (CIP-013).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Fundamentally, CIP-013 is a planning horizon standard to manage cyber security risks throughout the supply chain up to installation whereas the proposed requirements to CIP-005 and CIP-010 apply to applicable systems that are in-service in the operations horizons.	
Barry Jones - Barry Jones On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

1. The NERC SAR for this order is poorly written and inaccurate at best. The intent of the SAR is to communicate the ask, the specifics around what is required, and citations for the basis. Recommend revising the SAT to include the specific FERC Order and NERC technical paper requirements and recommendations. 2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The time period to comment on the SAR expired on 8/1/2019. The supply chain standards only consist of CIP-005, CIP-010 and CIP-013. Therefore changes to CIP-002 are not possible for the 2019-03 SDT.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Daniel Gacek - Exelon - 1	

Answer	
Document Name	
Comment	
Exelon is aligning with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 6.	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	

Comment
PG&E agrees with the EEI input on Question 6 regarding the modification to CIP-005-7, Requirement R2, Part 2.5 creating an untenable dilemma based on how it could be interpreted. This is based on the EEI comment of: "The language can be read to obligate entities to not just terminate vendor access through methods such as disabling rules within a firewall or disabling a user account for EACMS (e.g., Windows domain controller) but also to require entities to block all vendor access to the EACMS itself (i.e., install a firewall for the firewall)." EEI additionally indicated that if entities are required to block all access to the EACMS by installing a separate firewall, the newly installed firewall would be an EACMS which would then need to have another firewall installed creating an endless loop of new obligations. While the EEI recommendation indicates to remove EACMS from the Applicability Section of Requirement R2, Part 2.5, PG&E believes this would result in the modification not meeting FERC's directive in Order 850. PG&E recommends the Requirement language be modified to indicate the endless loop condition is not the intended purpose of the modification, or guidance be created which clearly indicates it is not the intended purpose of the Requirement. The preferred solution is Requirement language since Audit Teams are not bound to the wording in guidance.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see response to EEI in question 6. The SDT has moved CIP-005 requirements 2.4 and 2.5 to CIP-005 requirements 3.1 and 3.2 to provide clarity. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	

Comment	
FirstEnergy urges the SDT to develop Implementation Guidance for Industry review and comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has provided draft technical rationale and implementation guidance for all three supply chain standards along with this posting.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	
Document Name	
Comment	
CEHE supports the additional comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI for question 6.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

During our discussion with the SDT SME the SME indicated that mitigation would be required for CIP-013-2 R1 and TFIST request written clarification if mitigation will be required in CIP-013-2 R1. There is an error in the R3 moderate VSL that was carried over from the previous version. The existing text reads "…but has performed a vulnerability assessment more than 18 months …." However, it should read "but has performed a vulnerability assessment more than 18 months, but less than 21 months …."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2. The SDT has corrected the error in CIP-010-4 R3 moderate VSL.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports RSC comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT made minimal changes between CIP-013-1 and CIP-013-2 by adding EACMS and PACS. In response to the request for written clarification, please see ERO Enterprise staff responses to questions like this on CIP-013-1, in the Frequently Asked Questions Supply Chain – Small Group Advisory Sessions (p4, with response to R1.1) document dated June 28, 2018. The team believes these responses are still applicable to CIP-013-2. The SDT has corrected the error in CIP-010-4 R3 moderate VSL.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
Why are Protected Cyber Asset (PCA) or Protected Cyber System (PCS) per CIP [Definitions: Project 2016-02 Modifications to CIP Standards] not considered; given that the "impact rating of the PCA [or PCS] is equal to the highest rated BCS in the same ESP?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PCA's are not in scope for this SAR.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO	
Answer	
Document Name	
Comment	
Comments:	

1.) Recommend the SDT for Project 2019-03: Cyber Security Supply Chain Risks reach out to the SDT for Project 2019-02: BCSI Access Management to explore whether the vendor-related requirements currently proposed under Project 2019-02, i.e. CIP-011-3, requirement R1, part 1.4, "to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information," would be a better fit with the existing requirements under CIP-013 and, if so, discuss what would be needed to incorporate those changes into CIP-013-2. Additional support for exploring this recommendation is provided below, showing the divergence in language between the two SDTs. 2.) A SDT member indicated in conversation that mitigation would be required for CIP-013-2 requirement R1. The current language of CIP-013-2, R1, part 1.1, only requires an entity to "identify and assess cyber security risks;" there is no mention of mitigation. Conversely, the parallel SDT team working on Project 2019-02: BCSI Access Management has proposed language for CIP-011-3, requirement R1, part 1.4, that will require an entity to implement one or more documented information protection program(s) including "Processes to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information." We request the SDT, in order to avoid duplication of requirements across multiple standards, to collaborate with the SDT for Project 2019-02 to either: - Migrate all vendor-related requirements currently proposed under CIP-011-3, R1, Part 1.4 to CIP-013-2, OR - Drop any plans to introduce mitigation in CIP-011-3, R1, Part 1.4 and defer to the language in the existing, similar requirement under CIP-013-1, R1, Part 1.1. We believe the SDT has the latitude under the SAR to undertake this consolidation per the Project Scope: "This project will address the directives issued by FERC in Order No. 850. This project will also consider NERC staff recommendation from the Supply Chain Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements."	
Likes 1	Jones Barry On Behalf of: Rosemary Jones, Western Area Power Administration, 1, 6;

Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy suggests the following: Current CIP standards don't require entity to go beyond ESP boundary to monitor vendor remote access. Since all EACMS and PACS system don't reside within an ESP, the focus of this standard will shift beyond ESP boundary, where will be required to monitor and possibly terminate such access before such traffic even gets to ESP firewall. Duke Energy believes only EACMS or PACS devices that reside within an ESP should be the focus of this standard, so original intention of CIP-005 protection at the ESP level doesn't get derailed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. FERC Order 850 and the NERC Supply Chain Report did not specify only certain EACMS and PACS should be protected but all EACMS and PACS should be protected. The SDT drafted the standards to meet those requirements.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	
Document Name	
Comment	

We suggest moving revised CIP-011-2 R1.4 to CIP-013 R1.1 to address BCSI cloud services provider's risks since it really belongs to the supply chain risk management.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2019-03 team has had discussions with the Project 2019-02 team and understand that they are drafting changes to CIP-011-3. BCSI is not part of the SAR for Project 2019-03.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	
Document Name	
Comment	
FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.	
sean erickson - Western Area Power Administration - 1	
Answer	
Document Name	
Comment	
1. The NERC SAR for this order is poorly written please revise to include the FERC Order and NERC technical paper requirements 2. Consider revising CIP-002 to identify all different Cyber System and Cyber Asset types and their ability to be accessed locally and remotely (physical and electronic). Distinguish between EACMS and PACS which provide preventive and detective controls and identify internal controls which meet the audit requirements and are agreeable to industry	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The time period to comment on the SAR expired on 8/1/2019. The supply chain standards only consist of CIP-005, CIP-010 and CIP-013. Therefore changes to CIP-002 are not possible for the 2019-03 SDT.	
Marty Hostler - Northern California Power Agency - 5	

Answer	
Document Name	
Comment	
I feel FERC/NERC should be vetting Vendors and creating a list for us. Similar to Underwriter Labs (UL) reviewing, vetting, and testing equipment, then stamping it for appropriate use.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the SDT has passed this comment along to NERC compliance. CIP-013 including industry guidance for compliance with CIP-013 provides flexibility to use an independent assessment or third-party accreditation when vetting vendors.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to MRO in question 6.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Initial Ballot and Non-binding Poll Open through March 11, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Wednesday, March 11, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Balloting

Use the Standards Balloting and Commenting System (SBS) to submit votes. Contact Wendy Muller regarding issues using the SBS.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The results will be posted on the project page and announced when the ballots close. The drafting team will review all responses received during the comment period and determine the next steps of the project.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through March 11, 2020
Ballot Pools Forming Through February 25, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Wednesday, March 11, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Tuesday, February 25, 2020.** Registered Ballot Body members can join the ballot pools here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 2-11, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify "Project 2019-03 Cyber Security Supply Chain Risks Observer List" in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/189)
Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 IN 1 ST
Voting Start Date: 3/2/2020 12:01:00 AM
Voting End Date: 3/11/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 266
Total Ballot Pool: 300
Quorum: 88.67
Quorum Established Date: 3/11/2020 2:52:23 PM
Weighted Segment Value: 50.51

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	81	1	29	0.468	33	0.532	0	10	9
Segment: 2	6	0.6	2	0.2	4	0.4	0	0	0
Segment: 3	67	1	25	0.5	25	0.5	0	8	9
Segment: 4	20	1	9	0.529	8	0.471	0	1	2
Segment: 5	69	1	26	0.473	29	0.527	0	3	11
Segment: 6	46	1	18	0.462	21	0.538	0	5	2
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	1	0.1	0	0	0	2	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	1	0	0	0	0	0	0	1	0
Segment: 10	7	0.5	4	0.4	1	0.1	0	1	1
Totals:	300	6.2	114	3.131	121	3.069	0	31	34

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Third-Party Comments
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Wes Wingen		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Third-Party Comments
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	None	N/A
1	CMS Energy - Consumers Energy Company	Donald Lynd		Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Abstain	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Negative	Third-Party Comments
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Angela Gaines		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Allen Klassen		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Third-Party Comments
3	Cleco Corporation	Maurice Paulk	Clay Walker	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Abstain	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	Omaha Public Power District	Aaron Smith		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		None	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	Seattle City Light	Laurie Hammack		None	N/A
3	Seminole Electric Cooperative, Inc.	Michael Lee		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Westar Energy	Marcus Moor		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Jun Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Dwayne Parker		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Scott Tomashefsky		Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		None	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		None	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	Enel Green Power	Mat Bunch		Abstain	N/A
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Negative	Comments Submitted
5	Manitoba Hydro	Yuguang Xiao	Helen Zhao	Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		None	N/A
5	NaturEner USA, LLC	Eric Smith		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	James Mearns	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		None	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	Seattle City Light	Faz Kasraie		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	David Weber		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Westar Energy	Derek Brown		Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Colorado Springs Utilities	Melissa Brown		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil	Michael Lowman	Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Truong Le	Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nick Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Abstain	N/A
6	Omaha Public Power District	Joel Robles		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Westar Energy	James McBee		Negative	Comments Submitted
6	Western Area Power Administration	Rosemary Jones	Barry Jones	Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 300 of 300 entries

BALLOT RESULTS

Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 Non-binding Poll IN 1 NB
Voting Start Date: 3/2/2020 12:01:00 AM
Voting End Date: 3/11/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 246
Total Ballot Pool: 284
Quorum: 86.62
Quorum Established Date: 3/11/2020 3:14:47 PM
Weighted Segment Value: 47.12

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	74	1	23	0.469	26	0.531	15	10
Segment: 2	6	0.4	1	0.1	3	0.3	2	0
Segment: 3	66	1	18	0.439	23	0.561	14	11
Segment: 4	16	1	7	0.538	6	0.462	2	1
Segment: 5	67	1	21	0.457	25	0.543	9	12
Segment: 6	44	1	15	0.469	17	0.531	9	3
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	1	0.1	0	0	2	0
Segment: 9	1	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	4	0.4	1	0.1	1	1
Totals:	284	6	90	2.972	101	3.028	55	38

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Black Hills Corporation	Wes Wingen		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Comments Submitted
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	None	N/A
1	CMS Energy - Consumers Energy Company	Donald Lynd		Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Jose Avendano Mora		None	N/A
1	Eversource Energy	Quintin Lee		Abstain	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Angela Gaines		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sempra - San Diego Gas and Electric	Mo Derbas		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Allen Klassen		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Kent Feliks		Abstain	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Comments Submitted
3	Cleco Corporation	Maurice Paulk	Clay Walker	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Abstain	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
3	Great River Energy	Michael Brytowski		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	Omaha Public Power District	Aaron Smith		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		None	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Negative	Comments Submitted
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	Seattle City Light	Laurie Hammack		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seminole Electric Cooperative, Inc.	Michael Lee		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Marcus Moor		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
4	American Public Power Association	Jack Cashin		None	N/A
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
4	CMS Energy - Consumers Energy Company	Dwayne Parker		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		None	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Abstain	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		None	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NaturEner USA, LLC	Eric Smith		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		Negative	Comments Submitted
5	Pacific Gas and Electric Company	James Mearns	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		None	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	Seattle City Light	Faz Kasraie		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	David Weber		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
5	Westar Energy	Derek Brown		Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Colorado Springs Utilities	Melissa Brown		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil	Michael Lowman	Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Pool	Tom Reedy	Truong Le	Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Muscatine Power and Water	Nick Burns		Negative	Comments Submitted
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Abstain	N/A
6	Omaha Public Power District	Joel Robles		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Westar Energy	James McBee		Negative	Comments Submitted
6	Western Area Power Administration	Rosemary Jones	Barry Jones	Negative	Comments Submitted
8	David Kiguel	David Kiguel		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 284 of 284 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAMCS; 2. PACS; and 3. PCA	Have one or more methods for detecting vendor-initiated remote access sessions.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related

CIP-005-7 Table R3 – Vendor Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have one or more method(s) to terminate established vendor-initiated remote access sessions.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as: • PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate

CIP-005-7 Table R3 – Vendor Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			System. • PACS or EACMS Methods to disable active vendor remote access either through Electronic Access Point, an Intermediate System or any other method of remote access

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3)	The Responsible Entity did not have a method for detecting vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.1 for other applicable systems types (3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by 3.1 for PACS but did not have a method for detecting vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not have a method to terminate established vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.2 for other applicable systems types (3.2).	access sessions for other applicable system(s) types (3.1). OR The Responsible Entity had method(s) as required by 3.2 for PACS but did not have a method to terminate established vendor-initiated remote access sessions for other applicable system(s) types (3.2). OR The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and	OR The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			3.2 other applicable systems types. OR The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~2.4~~	~~1. High Impact BES Cyber Systems and their associated:PCA;~~ ~~2. PACS; and~~ ~~3. EACMS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. PCA;~~ ~~2. PACS; and~~ ~~3.~~1. ~~EACMS~~	~~Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).~~	~~Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:~~ ~~• Methods for accessing logged or monitoring information to determine active vendor remote access sessions;~~ ~~• Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or~~ ~~• Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.~~

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~2.5~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).~~	~~Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:~~ ~~• PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ ~~• PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~ ~~• PACS or EACMS Methods to disable active vendor remote access either through electronic access point, an intermediate system or any other method of remote acess~~

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management			
Part	Applicable Systems	Requirements	Measures

3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAMCS; 2. PACS; and 3. PCA	Have one or more methods for detecting vendor-initiated remote access sessions.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R3 – Vendor Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have one or more method(s) to terminate established vendor-initiated remote access sessions.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as: • PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System. • PACS or EACMS Methods to disable active vendor remote access either through Electronic Access Point, an Intermediate System or any other method of remote access

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3. ~~OR~~ ~~The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions for PACS (2.4); or one or more methods to disable active vendor remote access for PACS (2.5).~~	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; ~~OR~~ ~~The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive~~	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~OR~~ ~~The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions, excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access,~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Remote Access and system-to-system remote access) (2.5).~~ ~~OR~~ ~~The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions for PACS (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access for PACS (including Interactive Remote Access and system-to-system remote access) (2.5).~~	~~excluding PACS, (including Interactive Remote Access and system-to-system remote access) (2.5).~~
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3)	The Responsible Entity did not have a method for detecting vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.1 for other applicable systems types (3.1).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by 3.1 for PACS but did not have a	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3) OR The Responsible Entity did not have any methods as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The Responsible Entity did not have a method to terminate established vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.2 for other applicable systems types (3.2).	method for detecting vendor-initiated remote access sessions for other applicable system(s) types (3.1). OR The Responsible Entity had method(s) as required by 3.2 for PACS but did not have a method to terminate established vendor-initiated remote access sessions for other applicable system(s) types (3.2). OR The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2	required by Parts 3.1 and 3.2 (R3). OR The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types. OR The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.

- ~~Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').~~

~~The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.~~

~~For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.~~

~~If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.~~

~~The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.~~

~~This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.~~

~~As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.~~

~~The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.~~

~~Requirement R2:~~

~~See Secure Remote Access Reference Document (see remote access alert).~~

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

~~Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.~~

~~Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.~~

~~The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).~~

~~The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators~~

~~**Summary of Changes:** This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.~~

~~**Reference to prior version:** (Part 2.1) New~~

~~**Change Rationale:** (Part 2.1)~~
~~*This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*~~

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~ second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity. ~~except as provided in Requirement R1, Part 1.6.~~
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including ~~of~~ the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~*Note: The Guidelines and Technical Basis section and Rationale section has not been revised as part of Project 2019-03. A separate technical rationale document will be created to cover Project 2019-03 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Baseline Configuration~~

~~The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.~~

~~Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be~~

~~necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.~~

~~Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:~~

~~Asset #051028 at Substation Alpha~~

- ~~R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC~~
- ~~R1.1.2 – Not Applicable~~
- ~~R1.1.3 – Not Applicable~~
- ~~R1.1.4 – Not Applicable~~
- ~~R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823~~

~~Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.~~

~~Cyber Security Controls~~

~~The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in~~

those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007.

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a

~~plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:~~

- ~~Diagnostic test equipment;~~
- ~~Packet sniffers;~~
- ~~Equipment used for BES Cyber System maintenance;~~
- ~~Equipment used for BES Cyber System configuration; or~~
- ~~Equipment used to perform vulnerability assessments.~~

~~Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.~~

~~The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.~~

~~With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would~~

negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

~~including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).~~

~~Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.~~

~~Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.~~

~~Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.~~

- ~~Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.~~
- ~~Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.~~

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient

~~Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.~~

- ~~For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.~~
- ~~Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.~~
- ~~Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.~~
- ~~In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.~~
- ~~When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.~~

~~Requirement R4, Attachment 1, Section 2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.~~

~~To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.~~

- ~~Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.~~
- ~~Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.~~
- ~~Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.~~
- ~~When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.~~

~~Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

- ~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 – Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber

~~Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.~~

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for

~~these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes~~.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~ second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~January – March 2020~~
45-day formal comment period with additional ballot	May – June 2020
45-day formal comment period with second additional ballot	July – September 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

~~Link to the Implementation Plan and other important associated documents~~None.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

~~Rationale~~

~~*Note: The Rationale section has not been revised as part of the initial ballot for Project 2019-03. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Requirement R1:~~

~~The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):~~

~~(1) Software integrity and authenticity;~~
~~(2) Vendor remote access;~~
~~(3) Information system planning; and~~
~~(4) Vendor risk management and procurement controls.~~

~~The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.~~

~~Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).~~

~~Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.~~

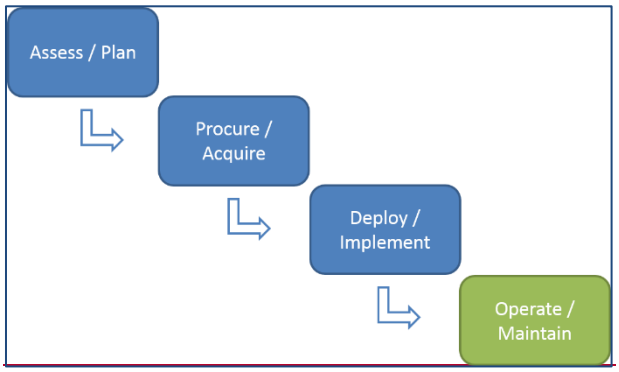
~~Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.~~

~~The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.~~

~~Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.~~

~~Notional BES Cyber System Life Cycle~~



~~Requirement R2:~~

~~The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).~~

~~Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:~~

- ~~NERC or the E-ISAC~~
- ~~ICS-CERT~~
- ~~Canadian Cyber Incident Response Centre (CCIRC)~~

~~Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all

applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18~~2~~ months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18~~2~~ months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6. The Implementation Plan associated with CIP-002-6 provides as follows~~The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5 shall apply to CIP-002-6. The Implementation Plan associated with CIP-002-5 provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard)~~:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber

System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-03 Cyber Security Supply Chain Risks

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-005-7, CIP-010-4, and CIP-013-2** by **8 p.m. Eastern, Monday, June 22, 2019.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

Project 2019-03 is in response to FERC Order 850 and the NERC Supply Chain Report to make modifications to the Supply Chain Standards, CIP-005-7, CIP-010-4, and CIP-013-2.

The NERC Supply Chain Report recommended including Electronic Access Control and Monitoring Systems (EACMS) that provide electronic access control and excluding monitoring and logging. The standard drafting team (SDT) considered excluding monitoring and logging. However, operationally classifying assets using multiple definitions under different requirement of the same standard, and from standard to standard, has the potential to create confusion and unnecessary complexity in compliance programs.

The NERC Supply Chain Report recommended including Physical Access Control Systems (PACS) and excluding alerting and logging. The SDT considered excluding alerting and logging. However, operationally dealing with separate functionalities within the same asset definition has the potential to create confusion within the other standards that reference the current PACS definition in the applicability column.

In conclusion, the SDT decided to use the currently approved glossary definitions of EACMS and PACS in modifications to the Supply Chain Standards. The currently approved glossary definitions are all inclusive of the functionality of the systems and do not separate any subset of functions. Any modification to the existing definitions would have a wide impact on the CIP Standards outside of the Supply Chain Standards.

Questions

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

3. The SDT is proposing removing the exception language in CIP-010-4 “Applicable Systems” for PACS which stated “except as provided in Requirement R1, Part 1.6.” This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

   ☐ Yes

   ☐ No

   Comments:

6. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

7. Provide any additional comments for the standard drafting team to consider, if desired

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirement R1

The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R1

The VSL did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R2

The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirement R2

The VSL is explained in the following pages.

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2, Requirement R1

The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R1
The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R2
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R2
The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.

VRF Justification for CIP-013-2, Requirement R3
The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirement R3
The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;~~OR~~ ~~The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system to~~	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~OR~~ ~~The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and~~

		~~system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).~~	~~system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).~~

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from the FERC approved CIP-005-6 Reliability Standard, with the following exceptions. In the high and severe VSL, the second levels are removed because Requirement R2 Part 2.4 and Part 2.5 have been removed from the standard language. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3)	The Responsible Entity did not have a method for detecting vendor-initiated remote access sessions for PACS but had method(s) as required by Part 3.1 for other applicable systems types (3.1). OR The Responsible Entity did not have a method to terminate established vendor-initiated	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by 3.1 for PACS but did not have a method for detecting vendor-initiated remote access sessions for other applicable system(s) types (3.1). OR	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3). OR The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
	remote access sessions for PACS but had method(s) as required by Part 3.2 for other applicable systems types (3.2).	The Responsible Entity had method(s) as required by 3.2 for PACS but did not have a method to terminate established vendor-initiated remote access sessions for other applicable system(s) types (3.2). OR The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types. OR The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)	methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs are based on the newly formed CIP-005-7 Requirement R3 which are modified from CIP-005-6 Requirement R2 Part 2.4 and Part 2.5. The Requirement R3 were modelled after the original CIP-005-6 Requirement R2 VSL's with the addition of PACS as an applicable system at a lower level than the other applicable system types listed in Requirement R3 Part 3.1 and Part 3.2.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2 which Requirement R3 is modified from.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium is consistent with Reliability Standard CIP-005-7 Requirement R3 which addresses Remote Access Management.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser- risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement~~s~~ R3~~2.4 and R2.5~~ and CIP-010-4 Requirement R1.6 ~~and~~ to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement~~s~~ R3~~2.4 and R2.5~~ and CIP-010-4 Requirement R1.6 ~~and~~ to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-7 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the second posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. The comparison below shows the modifications from CIP-005-6 Requirement 2 Part 2.4 and Part 2.5 to CIP-005-7 Requirement 3 Part 3.1 and Part 3.2.

CIP-005-6 Language	CIP-005-7 Language
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.1: Have one or more methods for ~~determining~~ detecting ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.2: Have one or more method(s) to ~~disable~~ terminate established ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT
Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

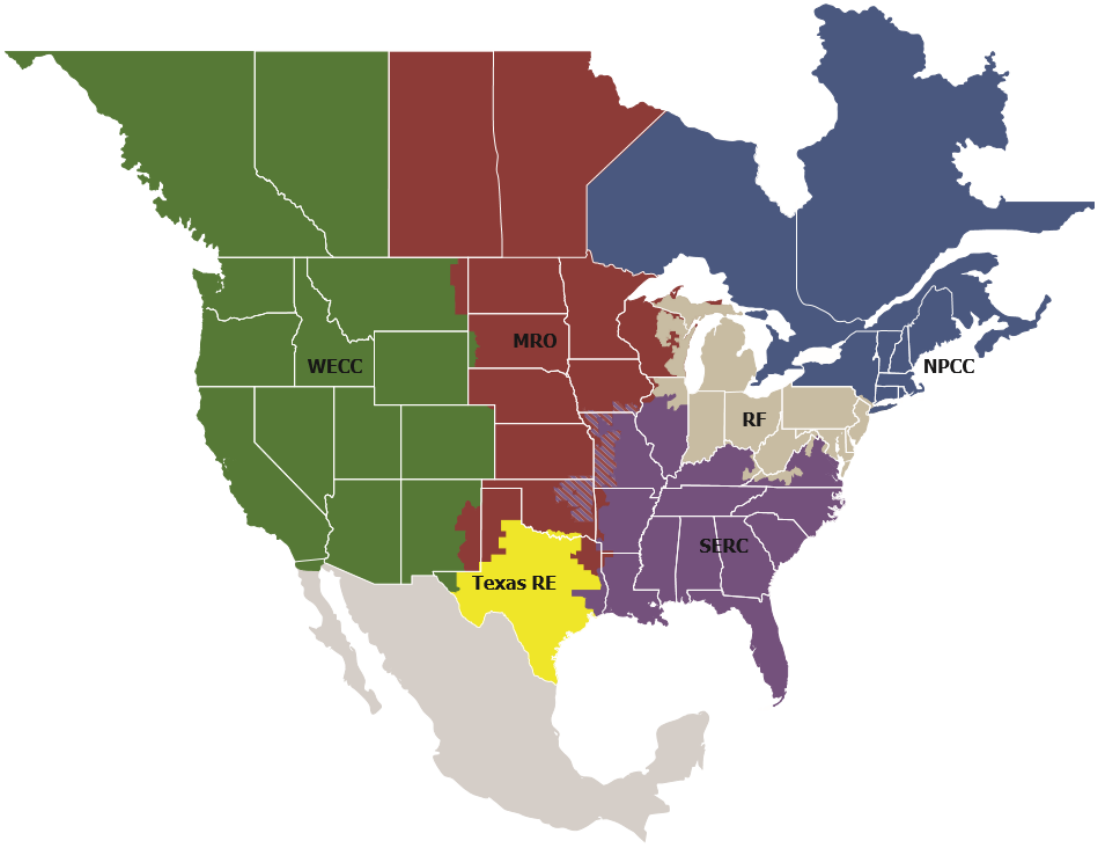
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risk Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement 3.1 and 3.2 Vendor Remote Access Management

The 2019-03 SDT added Requirement 3 to contain the requirements for all types of vendor remote access management. Additionally, the SDT added EACMS and PACS to the Applicable Systems for those requirements. EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow other to bypass authorization.

Since PACS devices potentially require physical presence to exploit, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus supporting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Precedent is set in CIP-006-6 Requirement R1 Part 1.5 on the importance of PACS by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that a compromised PSP poses imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

While other Reliability Standards mitigate certain security risks relating to PACS non address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only those control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACs), however if remote access is allowed, options to determine remote access session(s) and capability to disable remote access session(s) is required.

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

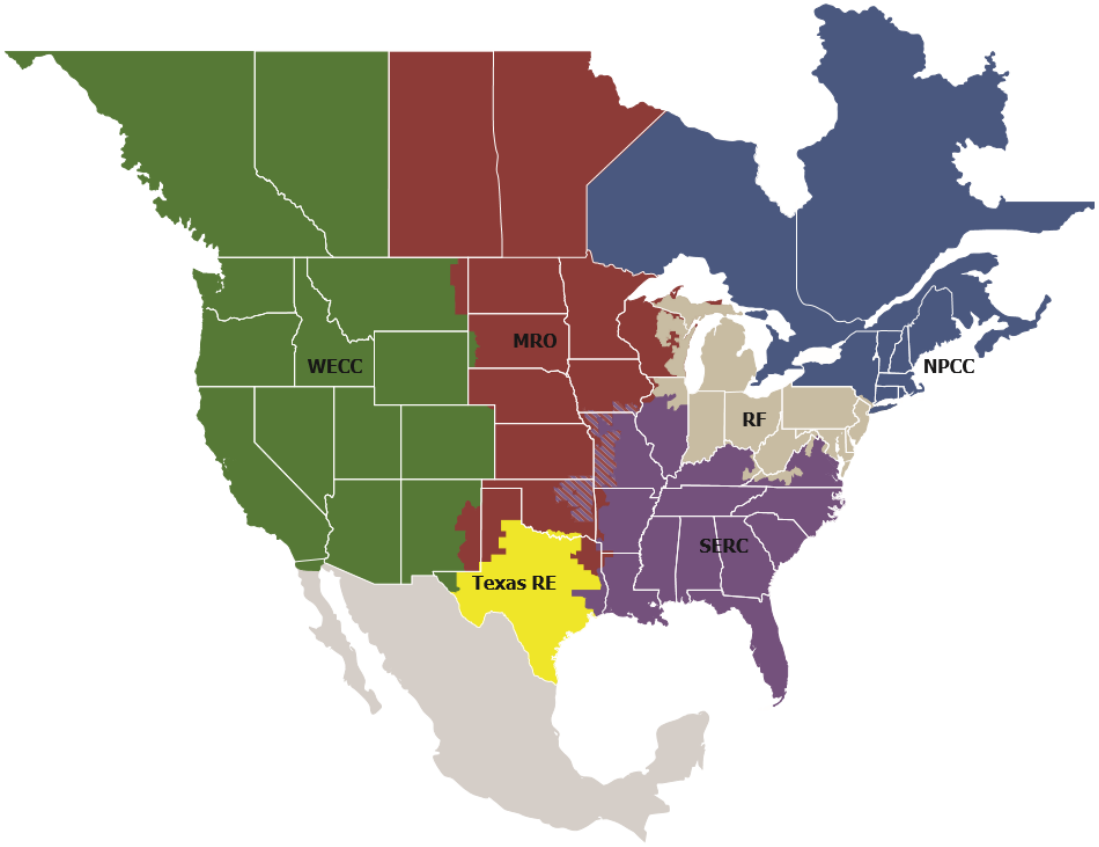
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rational for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

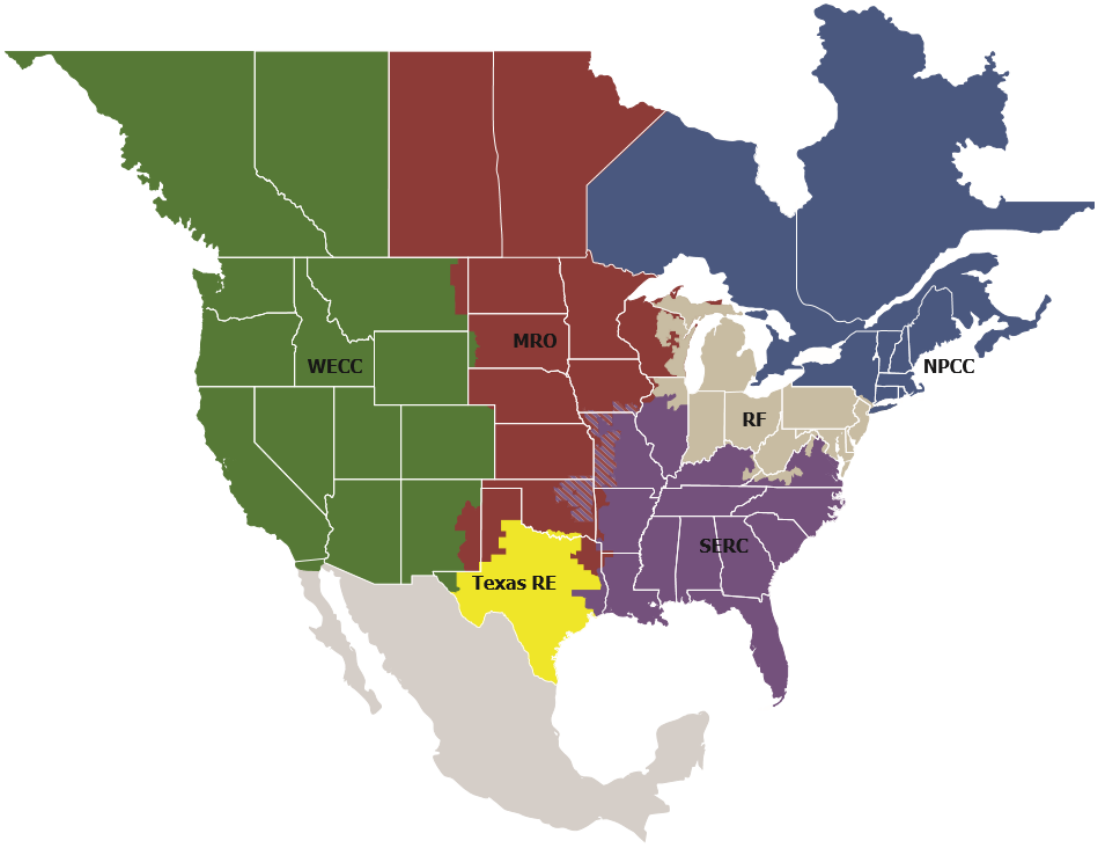
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

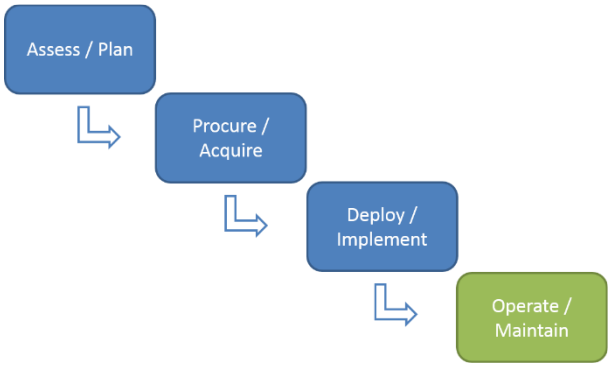
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2

General Considerations for Requirement R2

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

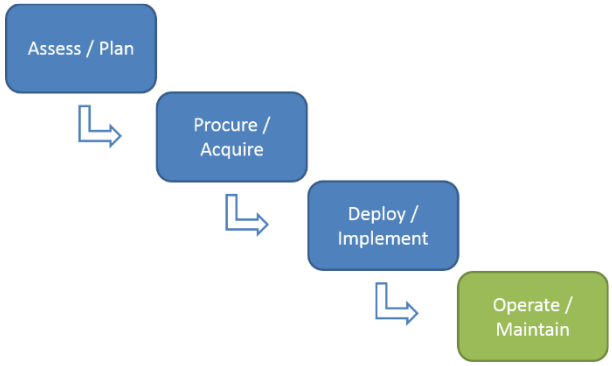
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

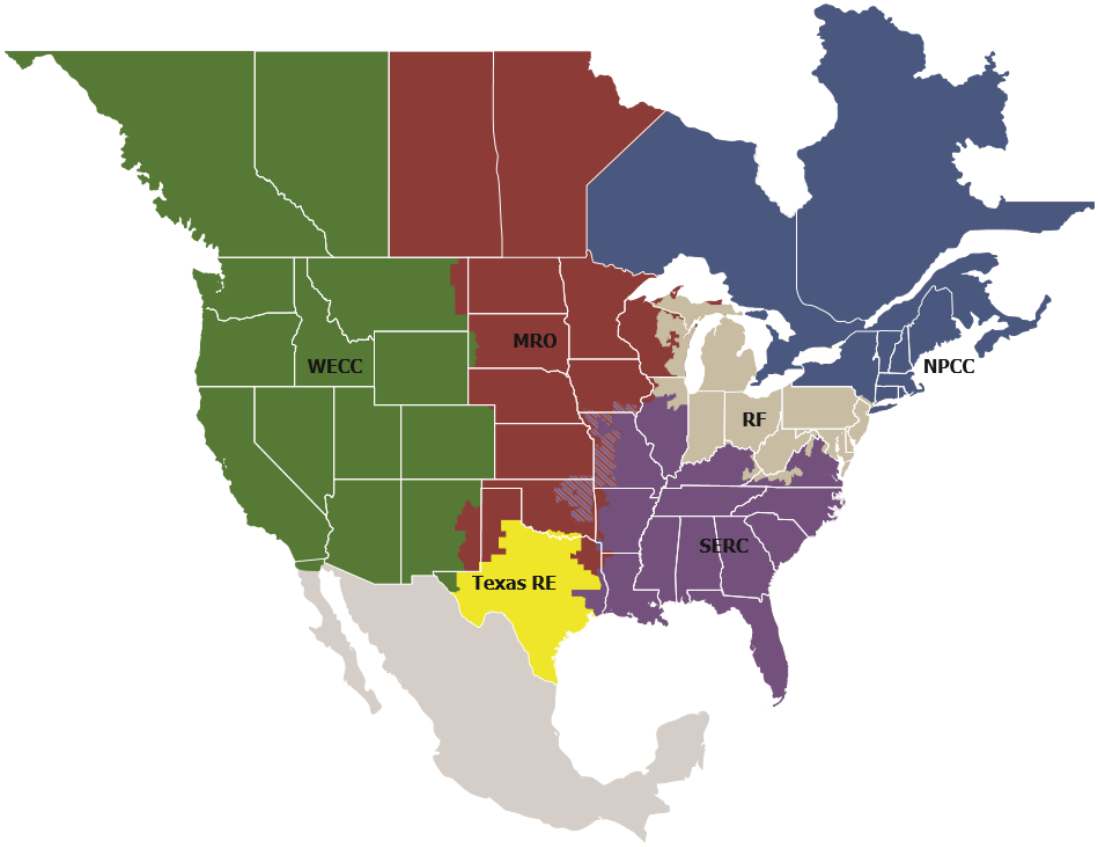
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management along with adding EACMs and PACs to the Applicable Systems column for Requirement parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method for remote access would be documented and the ability to disable that remote access would be required. For example, if an entity utilizes its corporate remote access solution to allow remote access into its PACS, the entity would need to document the remote access method, and develop a process to remove such access. Removing access may be as simple as disabling a token for that user account, or suspending or deleting that user's Active Directory account.

Since EAMCs are not a requirement for remote access to other EACMs the potential of the "hall of mirrors" issue is lessened (see above example). However, if an Entity uses the same system (Intermediate System for example) for remote access into both their BES Cyber Systems and their EACMS, the process of disabling remote access becomes tricky. Since the standard requires the removal of remote access to EACMS how can that be accomplished on the EACMs itself, the "hall of mirror" effect? For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the user attempts the remote access session, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disabled the user's ability to "access" the EACMs. The remote access user will "connect" with the EACMs however, the session will not allow "access" without the authentication methods being enabled, thus effectively not allowing remote access to that EACMS. This scenario shows a method to not allow remote access while eliminating the "hall of mirror" issue.

Where an entity strictly prohibits vendor remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations
2. An Entity could identify internal controls to periodically verify vendor remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture to provide supporting records that vendor remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-3 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes to baseline configurations that could lead to the introduction of vendor remote access to provide additional assurance that vendor remote access is prohibited as expected.
    e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-3 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations,

and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor remote access could be detected and reverted/revoked if established in violation of policy.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit . This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example , most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

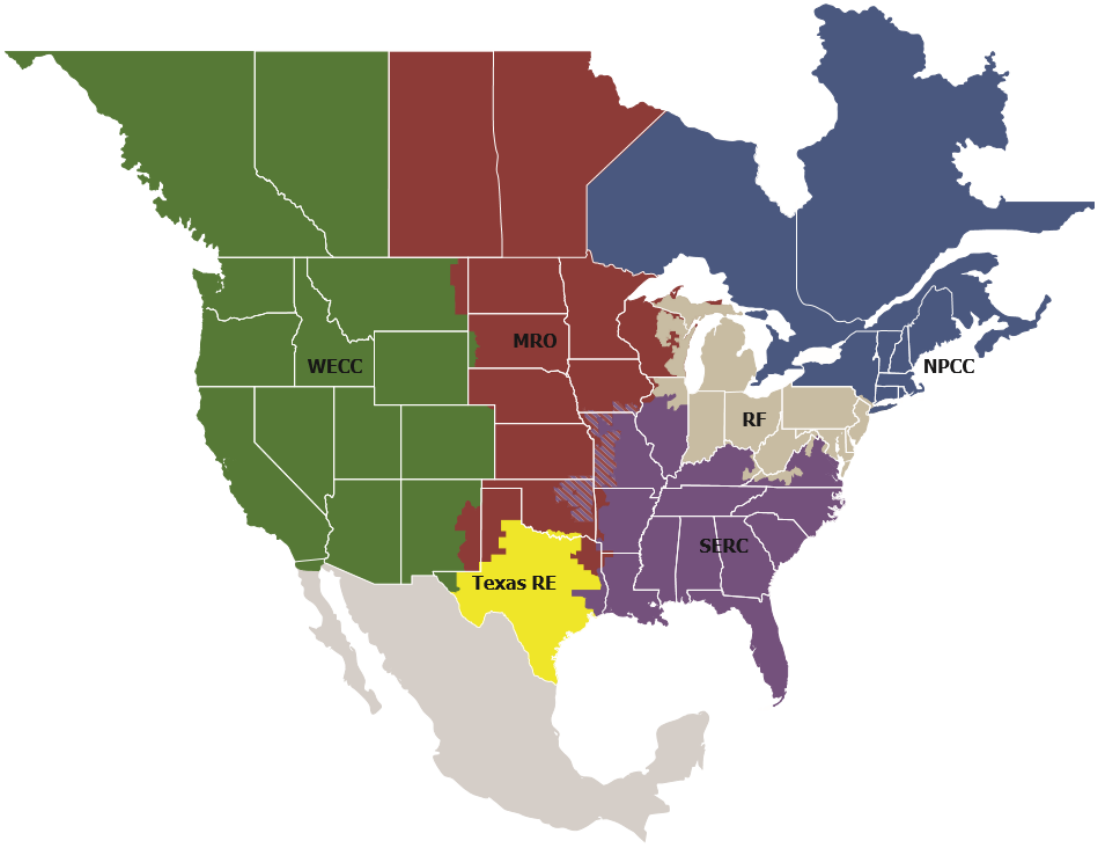
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT
Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-2

May 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report[1] recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2~~1~~ – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[2]~~.~~ and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2~~1~~ and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2~~1~~. Responsible Entities may choose alternative approaches that better fit their situation.

[1]NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2]Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated (i)~~Interactive R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-~~1~~2.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-~~4~~3, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems~~,~~ and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

  1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[3]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[4]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.

Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

[3]Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[4]For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[5].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

[5]An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.

  During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities

should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for ~~(i)~~ vendor-initiated (i) ~~Interactive~~ ~~R~~remote ~~A~~access, and (ii) system-to-system remote access ~~with a vendor(s)~~.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2~~1~~. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2~~1~~.

Requirement R3

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through June 22, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, June 22, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 12-22, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2 (Draft 2)
Comment Period Start Date:	5/7/2020
Comment Period End Date:	6/22/2020
Associated Ballots:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 2 ST

There were 75 sets of responses, including comments from approximately 183 different people from approximately 124 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

6. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. Provide any additional comments for the standard drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	Bobbi Welch	MISO	2	RF
					Ali Miremadi	CAISO	2	WECC
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO

					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	3		NIPSCO	Joe O'Brien	NiSource - Northern Indiana Public Service Co.	6	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Steve Toosevich	NiSource - Northern Indiana Public Service Co.	1	RF
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
Public Utility District No. 1 of Chelan County	Ginette Lacasse	1	WECC	PUD #1 Chelan	Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
					Ginette Lacasse	public Utility Distric No 1 of Chelan	1	WECC
	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1 of	4	WECC

Snohomish County PUD No. 1						Snohomish County		
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Alyssia Rhoads	Public Utility District No. 1 of Snohomish County	1	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Scott Brame	North Carolina EMC	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Meredith Dempsey	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
DTE Energy - Detroit	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF

Edison Company					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC

Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					John Pearson	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Jim Grant	NY-ISO	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					John Hasting	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable

					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Lower Colorado River Authority	Teresa Cantwell	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	

Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project.

More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures

For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

R2 states “For all Interactive Remote Access, utilize an Intermediate System”. However, by creating a new requirement specifically for vendor access there could be confusion that the access is “vendor” related access and R2 is not applicable. Based on the wording of this Question as context, it appears that it’s the intent of the SDT to remove intermediate systems for vendor initiated IRA. Thus explicitly allowing direct vendor access to assets in the ESP.

Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State recommends that CIP-005-7 R3 plane definitions be expanded, as they are brief and there is no further explanation of the planes in the Implementation Guidance or Technical Rationale. Suggest definitions similar to Cisco examples below:

1) Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network.

2) Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic. End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the

network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

The measures include as examples the usage of an EAP or Intermediate System to disable access. By the very nature of the devices, PACS and EACMS are outside of network boundary inclusion for CIP. To now require that termination of vendor access for EACMS and PACS by definition and available technology have required that controls be placed on these devices that contain assets outside of NERC CIP scope. EACMS and PACS should not be included in scope for Supply Chain management until or unless they are required to be placed behind a Firewall and required access via an Intermediate Server. The not do so leaves entities exposed to a wide interpretation during audit on what is an “acceptable” method for identification and termination of vendor access.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments

The changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard requires an Intermediate System to access an EACMS; and because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS.

The entity must implement another upstream control beyond that EACMS in order to disable the access “to” it, thereby creating another upstream device that qualifies as an EACMS by definition.

Recommend language to clarify the term access. This could be “authenticated access, access session, etc...” so it is clear that “a knock on the front door” of the EACMS that authenticates the system/user is NOT considered “access” (or in this case, by extension, “vendor remote access”) to an

EACMS. This would preclude auditors from interpreting a “knock at the front door of the EACMS that is later denied within the EACMS” as “access to” an EACMS.

Additionally, Requirement R3 Part 3.2 is a “how” in disguise instead of an objective “what”. Another potential solution to consider could be the following: Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access”. If this were the language, then “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the “knock at the front door” to the EACMS is no longer “access”.

Another consideration is to revise CIP-002 to allow entities to define only those systems they use as Intermediate Systems and/or Remote Access.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	
Comment	

Dominion Energy does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1, which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. In addition, the definition of EACMS currently includes Intermediate Systems. Based on these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. Additionally Dominion Energy continues to opine that EACMS should be excluded from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications included in this draft, has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

Dominion Energy is also of the opinion that “vendor remote access” includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because sSystems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity’s EACMS.

Dominion Energy is of the opinion that the SDT should consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	
Comment	

Reclamation recommends revising the language of CIP-005-7 R2 Part 2.1 to account for the addition of R3. It is not clear if Part 2.1 carries over and applies to R3.

Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Moving the language to the new R3 requirement does not make it clearer that Intermediate systems are not required for R3. If this is the SDT's intent, then it should directly state it in the requirement.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA notes that the proposed language still cites applicability to EACMS; Intermediate Systems are included in the definition of EACMS so the language still appears to include a requirement to determine active sessions to an Intermediate System, even if the remote session does not continue on the provide access to an asset in the ESP. In addition, not all EACMS are the same; this term has become too inclusive of many different types of technology to apply requirements. BPA believes the crux of the problem, as demonstrated by previous comments and unofficial ballot responses by multiple entities, is this: The EACMS definition is concurrently being modified by the 2016-02 project and keeping the current definition inclusive of logging and monitoring systems is problematic for the same reasons in both drafting efforts. The level of threat to and risk from a system that 'controls access' vs a system that provides a support function by 'logging or monitoring access and access attempts' is different. Logging and monitoring systems benefit from global oversight and gathering logs from the entire enterprise. Access granting systems benefit from specificity and narrow focus on the asset they are protecting. The CIP standards **must not** discourage or penalize efforts on the part of an entity to modernize their SIEM and threat analysis capability. Adding compliance burden to their enterprise logging and monitoring systems is such a discouragement.	

From a standards standpoint, this is not a common approach to address access control and access monitoring, as they are mutually exclusive. Even FISMA breaks them apart as control families as Access Control (AC) and Audit and Accountability (AU) to address access control and access monitoring respectively, as an example.

An example of more precise language (and BPA suggests this for inclusion in Guidelines and Technical Basis) might be:

R3.1 Have one or more methods for DETECTING active sessions (including both system-to-system and Interactive Remote Access, regardless of the identity of the person initiating the session) that traverse an EAP to logically access any applicable cyber asset in the ESP or ESZ.

R3.2 Have one or more method(s) to TERMINATE active sessions as referred to in R3.1

R3.3 Have one or more method(s) to DISABLE INITIATION OF NEW remote access sessions as referred to in R3.1.

Please note the terminology and conceptual change to a 3 part requirement: “Detect/Terminate/Disable”. The word “Determine” is unusual usage and not aligned with typical cyber security terminology. The reason for a separate requirement in our proposed R3.3 is simple; terminating existing sessions does not prevent an attacker from spawning new sessions, and it is very easy to automate such requests. The requirement to “disable active vendor remote access” is crippled by the word “active” because it does not clearly express a need to disable future sessions which are by definition not “active”. Combining the two requirements is parsimonious of words to the point of obscuring the objective. Without a means of denying new sessions, whether granularly or globally, an entity could find themselves playing “whack-a-mole” with an adversary and never able to manually keep it with automated requests. An example of granular control might be disabling a specific vendor’s remote access account, blocking requests from a specific IP address or range, or changing an authentication token or password for a particular user account’s remote access. This could be an absolute block or a suspension on new sessions for a timed period. For a global option, examples include simply denying all remote access attempts via change to a global VPN policy, firewall rule, etc. This is the proverbial “take a fire axe to the Internet connection” option.

The measures column for CIP-005=07 R3.1 includes *“Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.”* While this may be an effective measure for requiring authorization for a remote session, this is not an effective measure for determining an active session, sans a requirement to periodically/automatically terminate active sessions.

The measures column for R3.2 better captures the concept that the remote access to the Intermediate System or other EACMS is not the issue; simply getting a login prompt to a cyber-asset outside the ESP is low risk. Another means of clarifying the risk around Intermediate Systems might be to add Intermediate System to the applicability column to apply the R3.1 requirement to have a detective control, and leave it out of the R3.2(/R3.3 if adopted) applicability column, not requiring a specific ability to terminate/deny sessions to Intermediate Systems, but rather into the ESP/ESZ.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike

Answer	No
Document Name	

Comment

Tacoma Power thanks the SDT for considering our previous comments. Unfortunately, moving the language to a new requirement does not clarify the situation. Our concern is that the typical device used to detect a vendor remote access session is the EACMS that the vendor is accessing. Applying this requirement to an EACMS appears to be requiring an EACMS for an EACMS, producing a hall of mirrors.

Additionally, the term “active” has been removed from the language, removing this requirement’s role in support of the Part 3.2 requirement, since there is no time-bound nature to the current Part 3.1 language. We could have a method to detect after-the-fact vendor-initiated access, which would serve the Part 3.1 requirement language, but not the needs of Part 3.2.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

If intent is to specifically denote that intermediate systems are not required or in scope, suggest stating so directly: “Intermediate are not required for R3”.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

William Winters - Con Ed - Consolidated Edison Co. of New York - 5

Answer	No
Document Name	

Comment

Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project.

More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Oncor supports the comments submitted by EEI. In addition, without including the language that “Intermediate Systems are not required”, it is left to interpretation by the entity. In CIP-005-6, R2.1 and 2.2, use of an Intermediate System is clearly defined.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment
ATC thanks the SDT for attempting to resolve this concern, and agrees with the approach to separate this requirement out into R3; However, unfortunately the hall of mirrors condition still exists with EACMS in the applicability column due to a broader issue of ambiguity in the word “access”. Where getting “to” an EACMS associated with a high or medium impact BES Cyber System is considered “access” (or in this case, by extension, “vendor remote access”) the entity must still implement another upstream control beyond that EACMS in order to disable the access “to” it, thereby creating 1) another upstream device that qualifies as an EACMS by definition, 2) a hall of mirrors, and 3) an impossibility of compliance. ATC requests consideration of qualifying language that includes “authenticated access”, or something of the like, as the target instead of the ambiguous term “access” so it is clear that “a knock on the front door” of the EACMS that authenticates the system/user is NOT considered “access” (or in this case, by extension, “vendor remote access”) to an EACMS. This resolves the hall of mirrors issue and provides necessary specificity to preclude auditors from interpreting a “knock at the front door of the EACMS that is later denied within the EACMS” as “access to” an EACMS. Additionally, Requirement R3 Part 3.2 is a “how” in disguise instead of an objective “what”. Another potential solution to consider could be the following: Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. If this were the language, then “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the “knock at the front door” to the EACMS is no longer “access”.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
NV Energy supports EEI's comments.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	

Comment

The proposed changes dated 05/14/2020 do not provide clarity regarding the applicability of CIP-005 R2, which includes the need for an Intermediate System for **all** Interactive Remote Access Sessions. The requirement language does not distinguish between vendors vs. non-vendors; therefore, Intermediate Systems would be required for vendor Interactive Remote Access sessions.

Additionally, the current definition for Interactive Remote Access (IRA) in the NERC Glossary of Terms implies R1 and R2 may still be applicable to the new R3.

ISO-NE recommends that the SDT incorporate the new IRA definition proposed by the Virtualization SDT in Project 2016-02 Modifications to CIP Standards into this project. ISO-NE also recommends that the SDT return the language that was moved to the new R3 back to CIP-005 R2.4 and R2.5 in order to maintain continuity with the other CIP-005 R2 remote access requirement parts.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan

Answer	No
Document Name	

Comment

CHPD agrees with Tacoma Power, please refer to their comments.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern does not agree that the new R3 makes it clearer that Intermediate Systems are not required. In CIP-005 R2 Part 2.1, Intermediate Systems are required for ALL Interactive Remote Access sessions regardless of who initiates them. If the intent of this question is about clarity that terminating established vendor-initiated remote access sessions *to an Intermediate System* is no longer required, the answer is no. EACMS is in the Applicability column and the definition of EACMS is “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. **This includes Intermediate Systems.**” By the definition of EACMS, Intermediate Systems are still included in R3.

The proposed requirement would still require the ability to terminate vendor-initiated remote access sessions to the systems most often used to determine whether the session is vendor-initiated or not. Since the undefined term “vendor remote access” we believe includes both IRA and system-to-system access per the currently approved standard, it appears we would be required to determine the identity of the person BEFORE we allow their system to establish a session with our Intermediate System, which is not possible. The vendor's system must establish a session with the Intermediate System in order to even send the user credentials, which are then checked with usually yet another EACMS (such as a domain controller) in order to determine they are a vendor. At that point, the vendor's system has already had access to our EACMS.

We are also concerned about what “remote” means in context of an EACMS such as an Intermediate System. The definition of Intermediate System states it must NOT be located inside an ESP. The Intermediate System is already remote according to most definitions of remote (‘outside the ESP’) so what is remote to a remote system?

Southern believes for these reasons that EACMS should either not be in the scope of these particular CIP-005 requirements and the security objective is to be able to determine and disable vendor remote access sessions to BES Cyber Systems *by using EACMS to do so*. If there is some other vendor EACMS access that is intended, it should be precisely described and used within a separate requirement from the main objective of protecting the BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We do not believe this requirement is clear with respect to Intermediate Systems. For any Interactive Remote Access, an Intermediate System should be required, no matter the source (vendor vs. internal).

Second, the second bullet in the measures for Part 3.1 discusses monitoring remote activity, which is inconsistent and exceeds the requirement to detect remote access sessions.

Third, the third bullet in the measures for Part 3.1 needs to better explain the methodology the SDT is intending to describe.

Lastly, the SDT is making an arbitary distinction for vendor remote access that is unnecessary. All remote access (vendor or internal) should be similarly treated in terms of detecting and termination. However, as discussed previously, the expectation for monitoring is not part of the identified requirements and should be removed from the measures.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	
Comment	
We appreciate the SDT efforts. However, this does seem to create a "hall of mirrors" as pointed put by a number of commentors by requiring an intermediate system for an intermediate system. There should also be allowance for CIP exceptional circumstances in CIP-013.	
Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated. Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	

Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated. Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST does not agree that the desired clarity has been achieved, especially since for certain types of “vendor remote access,” (e.g., Interactive Remote Access to applicable BES Cyber Systems), Intermediate Systems ARE required. Likewise, for user-initiated remote access, vendor or otherwise, to EACMS and PACS systems that happen to be within Electronic Security Perimeters (not altogether uncommon), Intermediate Systems ARE required. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of “vendor remote access” that require Intermediate Systems and types of “vendor remote access that do not, as CIP-005 is currently written, require Intermediate Systems:

Intermediate System required: Vendor remote access that meets the current NERC definition of “Interactive Remote Access” and is therefore subject to CIP-005 R2.

Intermediate System not required: Vendor remote access that does not meet the current NERC definition of “Interactive Remote Access.” This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable.

One way to address this might be to break R3 part 3.1 into two sub-parts:

Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2).

Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.

Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

The changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard begs the question if an entity now needs another EACMS Intermediate System to access an EACMS? Because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS. The entity must implement another upstream control beyond that EACMS in order to disable the access “to” it, thereby creating another upstream device that qualifies as an EACMS by definition.

Personnel (employees, vendors, suppliers, contractors, etc..) need to be defined in CIP-004. Systems (vendor or entity owned and maintained) need to occur in CIP-002. Why not revise CIP-002 and allow entities to define only those systems they use as Intermediate Systems and/or Remote Access? Or vendor systems?

Why not revise CIP-004 to address vendors?

Additionally, Requirement R3 Part 3.2 is a “how” in disguise instead of an objective “what”. Another potential solution to consider could be the following: Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access”. If this were the language, then “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the “knock at the front door” to the EACMS is no longer “access”.

Secondly, the standard does not clearly define what System to System remote access is. A valid definition for system to system remote access needs to be created and added to the Glossary of Terms.

Lastly, Requirement 3 also conflicts with Requirement 1 part 1.3. If a Responsible Entity (RE) determines that a connection to a vendor is needed and has placed the appropriate controls on the appropriate interfaces of its protecting asset(s) (Firewalls, routers, etc..) then the connection is needed. Secondly the RE is responsible for determining if a vendor has adequate security controls in place or has applied mitigations as part of their CIP-013 process for that vendor then the requirement 3 is not needed. Connections made from a vendor (type, duration and need) should be spelled out in the procurement contracts derived out of the CIP-013 processes.

Likes 0	
Dislikes 0	

Response

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez

Answer	No
Document Name	

Comment

If intent is to specifically denote that the intermediate systems are not required or in scope it should be specifically stated “Intermediate systems are not required for R3”

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

Puget Sound Energy supporte the comments of EEI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 1.

Likes 0	

Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment
The removal of the term “interactive” and the retention of the terms “remote access” alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term “remote access” is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. For this reason, GTC/GSOC do not agree that the proposed revisions makes it clearer that Intermediate Systems are not required. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
In our opinion the original language in CIP-005-6 stating vendor remote access as system-to-system and interactive is clear and encompassing of all vendor remote access. No change is required to further clarify use of an Intermediate System. However, if further clarification that an Intermediate System is not required I propose the following: "Have one or more methods for determining active vendor remote access sessions (including system-to-system remote access, vendor initiated system-to-system remote access with or without use of an Intermediate System as well as Interactive Remote Access)."

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	

Comment

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that “vendor remote access” includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity’s EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition of change needs to happen as part of this project.

More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures

For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO, in general, supports the comments submitted by NPCC and by IRC The wording of Requirement R3 suggests that these are only requirements that apply to vendor initiated remote access and may miss the embedded requirement in Requirement R2. IESO recommends that the wording of Requirement R2 should explicitly add “including vendor initiated interactive remote access” as reminder that there are additional requirements for vendor initiated remote access outside of Requirement R3 While it is preferred, from a cyber-security perspective, to utilize an intermediate system for vendor initiated interactive remote access to EACMS and PACS, IESO recognizes that it may not be appropriate in all situations	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	No
Document Name	

Comment

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that “vendor remote access” includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity’s EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

MidAmerican supports EEI comments.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MidAmerican supports EEI comments.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

The removal of the term “interactive” and the retention of the term “remote access” (now, undefined) alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term “remote access” is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply as discussed below in GSOC’s and GTC comments in response to Question 2. For this reason, GSOC and GTC does not agree that the proposed revisions make it clearer that Intermediate Systems are not required. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

The NERC definition of Electronic Access Control or Monitoring Systems clearly states that Intermediate Systems are also considered as EACMS. Recommend specific language to address “Electronic Access Point(s)” for system to system remote access and intermediate systems for vendor IRA. It is inferred, however, not clear, that an Intermediate system is not required for system to system access, but is needed for IRA.

Separating the two parts into another requirement would make it clearer, however in R2.1 the requirement still reads that for **all** Interactive Remote Access, utilize an intermediate system. Somehow it still creates confusion if it’s required for “all” but not for vendors? In Requirement R2, Part 2.1, revise “all” remote sessions must be through an Intermediate System and add “excluding vendor system to system remote access through an EAP.”

Additionally, the requirement R3 Part 3.1 states “to detect” vendor-initiated remote access sessions. In the Examples of evidence, “Methods for accessing logged or monitoring information…” implies that the Responsible Entity is required to monitor vendor activity during the remote session. Is the objective to detect or to monitor the vendor remote access session or both? For instance, once the vendor remote session is detected or established, is the Responsible Entity required to monitor the vendor activity continuously during the remote session or just receive periodic alerts that the session remains open with the ability to terminate as needed?

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020

Answer	No
Document Name	

Comment

The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP includes Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter.

For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside of the ESP as the proposed language introduces an unsolvable problem.

Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013.

Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is supporting the IRC SRC Comments as follows:

The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP include Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter.

For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside the ESP as the proposed language introduces an unsolvable problem.

Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013.

Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

R2.1 states that an Intermediate System is required for all IRA. Vendor access is not excluded. Moving vendor access from Part 2 to Part 3 does not change that R2.1 is required. SRP recommends language in the standards are made clearer to indicate Intermediate Systems are not required in R3

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports the NPCC Regional Standards Committee comments.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4

Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the proposed modifications in CIP-005-7 makes it clearer that Intermediate Systems are not required.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to move all Vendor Remote Access requirement remote access from Parts 2.4 & 2.5 to Parts 3.1 and 3.2 since it is clearer that Intermediate System is not required for Interactive Remote access to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

The addition of the Applicable Systems to the Requirement Parts (by itself) makes it clear that Intermediate Systems are not required for vendor remote access; some of these applicable systems cannot reside in a defined Electronic Security Perimeter. The term “vendor-initiated” is troubling because it should not matter whether the vendor or the entity initiates the connection; the risks are identical either way. By specifying only “vendor-initiated” connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement. WECC recommends removing the term “vendor-initiated” to ensure risks of vendor access connections are addressed, whether vendor or entity initiated.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

While this does make it clearer, as a part of the standard’s Supplemental Material this should be spelled out, so there is no gray area.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Randy Cleland - GridLiance Holdco, LP - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	
Document Name	
Comment	

Texas RE agrees an additional Intermediate System is not needed for access to an EACMS Intermediate System, and that the SDT's addition of a new Requirement R3 clarifies this fact. Texas RE notes that, as presently drafted, the proposed Requirement R3 does not require multi-factor authentication and encryption for PACS and EACMS. Vendor remote access brings an increased risk of threats and vulnerabilities to registered entities' CIP environments. For example, a malicious actor could gain access to and/or control of the EACMS and PACS for multiple registered entities through a single compromised vendor. Requiring multi-factor authentication and encryption controls would help decrease the risk of misuse, compromise, and data breach through vendor remote access sessions.

As such, Texas RE suggests that the SDT consider incorporating multi-factor authentication and encryption requirements into the proposed Requirement R3. Alternatively, the SDT could implement these requirements by adding PACS and EACMS to the Applicable Systems subject to Requirement R2, Parts 2.1 – 2.3, while retaining the proposed Parts 2.4 and 2.5 from Draft One and incorporating clarifying language explaining that when an Intermediate System is an EACMS, another Intermediate System is not required.

Likes 0	
Dislikes 0	
Response	

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports the NPCC Regional Standards Committee comments.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

There is no definitive definition of what is an active vendor remote access session including system-to-system remote access as well as Interactive Remote Access, which includes vendor-initiated sessions.

SRP would like to see clear definitions added to the Glossary of Terms and examples of each within the Guidelines and Technical Basis.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

CIP-005, R3.1

“Detecting” is not a good word choice. Malicious traffic must be detected because it requires investigation and discovery. Vendor remote access is granted by the entity and the entity provides the method by which remote access is performed. The method enabling remote access must have the ability to enumerate remote access sessions.

Suggestion: The method enabling vendor-initiated remote access must have the ability to enumerate connected remote access sessions.

CIP-005, R3.2

An “established vendor” is a vendor that has been in business or a long time. How long does a session have to be active before it is widely considered to be established? The intent is to terminate a “connected” session.

Suggestion: Have one or more method(s) to terminate connected vendor-initiated remote access sessions.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

It isn’t as clear as it could be. Diagrams of the different scenarios would certainly help to clarify.

Additionally, suggest replacing the word “Detect” as this implies the vendor is trying to make a remote connection without any permission from the Responsible Entity. Suggested wording for R3, Part 3.1: Have one or more methods for “establishing and monitoring” vendor-initiated remote access sessions.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term “remote access” is not defined and could be construed as access from outside an entity’s network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor

and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GSOC and GTC recommends that the SDT either: (1) collaborate with the appropriate, assigned SDT to modify the definition of "Interactive Remote Access" as necessary to ensure that it incorporates the necessary language or (2) create newly defined terms for "vendor-initiated remote access" and "vendor-initiated system-to-system access." GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited.

Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

As written, see comments to question 1.

Likes 0	
Dislikes 0	

Response

Ray Jasicki - Xcel Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Support the comments of the Edison Electric Institute (EEI)

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	No
Document Name	

Comment
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited. Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
See response to question 1.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	

Comment
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	
Comment	
The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term “remote access” is not defined and could be construed as access from outside an entity’s network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	

Response	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

The term “detecting” in part 3.1 - whereas an entity is required to “Have one or more methods for **detecting** vendor-initiated remote access sessions” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” when they access the BCS. What is the security value in detecting a vendor who is already authorized to access the BCS?

A person accessing a system, vendor, or other should be addressed in CIP-004. The identification of a vendor system should occur in CIP-002. This also maps to ISO and NIST cyber security frameworks.

Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations a need may arise for vendors to initiate and establish remote access to an entities BCS, however a voice call to authenticate may be a better control.

Secondly, the words “established sessions” are an improvement from the language in the first draft; however, while this solved the problem posed by “disabling active sessions” where an idle session could remain enabled, it created another gap through the introduction of the word “initiated”. The qualifier “initiated” may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” and “capability to use” the established session that is the risk regardless of which end initiated it.

Recommend alternative language that focuses on the risk itself or consider : Requirement R3 Part 3.1. “Have one or more methods for detecting established vendor remote access sessions.” Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. In this case “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language.

Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket.

Consider language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005

Likes 0	
Dislikes 0	

Response
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	No
Document Name	
Comment	

N&ST does not agree that the desired clarity has been achieved. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of “vendor remote access” that DO require Intermediate Systems and types of “vendor remote access that do NOT, as CIP-005 is currently written, require Intermediate Systems:

Intermediate System required: Vendor remote access that meets the current NERC definition of “Interactive Remote Access” and is therefore subject to CIP-005 R2.

Intermediate System not required: Vendor remote access that does not meet the current NERC definition of “Interactive Remote Access.” This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable.

One way to address this might be to break R3 part 3.1 into two sub-parts:

Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2).

Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	
Comment	

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	
Comment	

As written, see comments to question 1

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

Oklahoma Gas & Electric supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

As written, see comments to question 1

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

The proposed revisions do not clearly define the types of remote sessions that are covered by the standards. CIP standards need to use consistent language, define unclear terms and not leave so much to interperetation if requiring specific actions.

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Refer to responses to Question 1.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree that the changes clearly define the types of remote sessions. There is still some ambiguity on what would be considered remote if the entity is to disable remote access to the very things that are used to define what remote access actually is. Would a remote user who attempts to get to an asset but is not authenticated and authorized, but made it to the asset that denies access, is that still considered access? The security which denies the access, such as a firewall, simply does not allow the access. However, there would be a log that is collected of the attempted access as well as any access that is authenticated and authorized.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

The proposed changes do not provide clarity. Although the addition of “initiated” is appreciated, the removal of the IRA and system-to-system qualifiers introduces ambiguity. It is unclear whether “all” remote access sessions must be included or if the Entity has the authority to define “vendor-initiated remote access sessions,” potentially reducing the scope of requirement.

The removal of IRA and system-to-system is also inconsistent with the language changes to CIP-013-2, R1.2.6.

Additionally, the “Measures” were not updated to reflect the proposed changes.

Specifically, the “Measures” still include the language from the original CIP-005-2 R2.4 and R2.5 requirements “active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access.”

ISO-NE recommends keeping the “initiated” qualifier, adding terms or information to clarify the specific in-scope remote access sessions, and ensuring consistency with CIP-013-2.

Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

NV Energy supports EEI's comments.

Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

ATC agrees the words “established sessions” are an improvement from the language in the first draft; however, while this solved the problem posed by “disabling active sessions” where an idle session could remain enabled, it created another gap through the introduction of the word “initiated”. The qualifier “initiated” may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” and “capability to use” the established session that is the risk regardless of which end initiated it. ATC requests consideration of alternative language that focuses on the risk itself. Another potential solution to consider could be the following: Requirement R3 Part 3.1. “Have one or more methods for detecting established vendor remote access sessions.” Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. If this were the language, then “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language.

Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket. ATC requests consideration of qualifying language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005.

Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD agrees with Tacoma Power, please refer to their comments.

Likes 0	
Dislikes 0	
Response	

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	No
Document Name	
Comment	
Oncor supports the comments submitted by EEI. In addition, there is a conflict between the language in CIP-005-7, R3 and CIP-013-2 inasmuch CIP-013, R1.2.6 takes out “Interactive”, and “with a vendor” in terms of remote or system to system access, but then the changes to CIP-005-7 do not match the changes in CIP-013-2, R1.2.6.	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
The changes to the newly formed R3 appear to have had the opposite effect of clearly defining the types of remote sessions. With these changes, there is no clarity about what a vendor-initiated remote access session is. Does “access” refer to read-only access? Or does “access” only refer to control? What is the meaning of “remote” in this situation? “Remote” to an applicable system? How is that clarified? Tacoma Power does not support these changes to CIP-005 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
While the SDT is coming at this from the supply chain aspect, the technical application of the mechanisms to detect, terminate and disable remote access sessions requires the ability to do it for any remote access session; therefore the specific language “active vendor remote access” and “includes vendor-initiated sessions” is of no practical value. If the entity has the ability to detect, terminate, and disable remote access sessions, they have the ability do this for vendors or for insiders. In BPA’s opinion, there is no point in making the requirement strictly about vendors. It could as easily be applied to partners, customers, remote employees, etc., and to the same benefit in reduced risk to the reliability and secure operation of the grid.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
No, Santee Cooper does not believe that the changes in CIP-005-7 R3 clarify remote session conditions. If this is the SDT’s intent, then they should define vendor-initiated remote access. In CIP-013-2 two different remote access conditions are mentioned vendor-initiated remote access and system to system remote access. Whereas in CIP-005-7 only vendor-initiated remote access is mentioned.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not equate to the device being exploited.	

Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments	

The term “detecting” in part 3.1 - whereas an entity is required to “Have one or more methods for **detecting** vendor-initiated remote access sessions” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” when they access the BCS. What is the security value in detecting an entity which is assumed to already be authorized to access the BCS?

Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations, a need may arise for vendors to initiate and establish remote access to an entity's BCS, however, a voice call to authenticate may be a better control.

Secondly, the words “established sessions” are an improvement from the language in the first draft; however, while this solved the problem posed by “disabling active sessions” where an idle session could remain enabled, it created another gap through the introduction of the word “initiated”. The qualifier “initiated” may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” and “capability to use” the established session that is the risk regardless of which end initiated it.

Recommend alternative language that focuses on the risk itself or consider: Requirement R3 Part 3.1. “Have one or more methods for detecting established vendor remote access sessions.” Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. In this case “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language.

Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read-only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket.

Consider language to exclude non-persistent read-only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

No, the changes made it worse by including the definition of a session in the measure and not in the requirement itself. As written in part 3.1 entities have to detect “vendor-initiated remote access sessions” without indication on what this includes. It is vague language. In the measure a definition is given for an active vendor remote access session as “including system-to-system, as well as interactive remote access, which includes vendor-initiated sessions”. Requirements cannot be buried in glossary definitions or measures as it implies a rule without be an explicit rule. The definition needs to be placed back into the requirement itself.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	

Comment
The Measures detailed in the Requirement Parts do clearly define the types of remote sessions that are covered by the standards. However, the Measures language does not use the same terminology (“vendor-initiated” connections) that is used in the Requirements language, which may lead to confusion. WECC recommends removing the term “vendor-initiated” as discussed in the previous comment.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
Tri-State does find the addition of the phrase "vendor-initiated" helpful, however we think it still leaves too much room for interpretation. To further clarify, we recommend a few additional edits: 1) In the measure for part 3.1, recommend changing the language “(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)” with “(either via system-to-system remote access or Interactive Remote Access, and which is initiated from a vendor’s asset or system)”, and 2) In the requirement itself, we recommend adding something like the following to end of the drafted requirement language ", whether via system-to-system remote access or Interactive Remote Access." Similar edits should be made to part 3.2. Finally, we ask that the drafting team consider adding a statement to help clarify and address the various emerging regional interpretations regarding web conferences, either in the core requirement R3, or under both parts 3.1 and 3.2. To that end, we recommend adding a statement to this effect "Remote sessions initiated by the responsible entity's personnel, where the vendor has no control, is not in scope".

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
This project should be canceled or at least placed on hold until the following occur: 1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is. 2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on. 3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA. 4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The words "vendor-initiated remote access sessions" are not properly defined and are ambiguous. "Sessions" could be taken as exclusive to TCP Only connections or could mean any connection such as a serial HyperTerminal session … etc. R2 strictly discusses vendor-initiated remote access. If an entity initiates the remote access via a WebEx and gives control to a vendor the access should then be considered vendor initiated and follow R3 requirements. Does the vendor-initiated remote access include non-routable vendor-initiated communications Consider including communications such as dial-up, serial, corporate TTY terminal servers to EACMS and PACS, etc.. Perhaps modify requirements to state P3.1 – " Have one or more methods for detecting all vendor sessions, regardless of protocol, type of connection, or initiation" and P3.2 - "Have one or more methods to terminate all vendor sessions regardless of protocol, type of connection, or initiation"

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 6

Answer	No
Document Name	

Comment

As written, see comments to question 1.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree that the proposed language clarifies remote session conditions. Duke Energy, is concerned about the new wording for R3.1, specifically the change of “determined” to “detecting”. This leaves open a question if the intent is continuous monitoring for or detection of sessions, on-demand or periodic detection, or just detection upon initiation.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding “vendor-initiated…”.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020

Answer	Yes
Document Name	

Comment
The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding “vendor-initiated…"

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to the proposing language in Part 3.2, but disagree the term “detecting” in Part 3.1 since “detecting” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” them. We suggest changing from “detecting” to “verifying”.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments to #1.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	

Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Question does not address the proposed addition of EACMS and PACS to the CIP-10-3 R1.6 requirement. ISO-NE does not agree with adding EACMS and PACS to the “Applicable Systems.” The additions potentially exceed the FERC order, which can be interpreted to only extend the supply chain requirements to the CIP-013-1 Standard. Given the CIP-010-3 R1.6 requirement is not even effective yet, there is insufficient evidence to support further expansion into a CIP environment.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC/GSOC do not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GTC/GSOC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GTC/GSOC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GTC/GSOC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	

Support the comments of the Edison Electric Institute (EEI)

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC and GTC does not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC asserts that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC remains opposed to the inclusion/addition of PACS to the applicable supply chain reliability standards. While GSOC and GTC understands the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, we believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020

Answer	No
Document Name	

Comment

The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose.

Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013.

Also, too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.

The IRC SRC believes that requirement R1.6 should be applied to other Cyber Assets. Making a regulatory compliance requirement for a subset of assets in the enterprise increases the cost of implementation and maintenance dramatically to a point that it may be detrimental to the overall company security posture, ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS and PACS to the R1.6 requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Also, it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven. it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes

Document Name	
Comment	
Duke Energy agrees with reverting the language in this section back to what is in CIP-010-3.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to remove the specific language in the Background section to clarify the applicable PACS.	
Likes 0	
Dislikes 0	
Response	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment
Seattle City Light concurs with the comments provided by Snohomish PUD

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
BPA agrees that this reads better with the language removed. However, if we are looking at this from a Supply Chain perspective perhaps we should consider removing with “External Routable Connectivity” and evaluate all PACS as they are being procured.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	

Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
No additional comments on this question.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern does not have any issues with the removal of the exception language in the Applicable Systems for PACS.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Answer should have been "No". We do not su[pport adding PACS.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6 We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

The redline-to-last-posted does not show any changed to Part 1.6

We agree that the SDT followed the Directive's instructions

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	

Comment

Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

The redline-to-last-posted does not show any changed to Part 1.6.

We agree that the SDT followed the Directive's instructions.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree that the SDT followed the Directive's instructions.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG supports the NPCC Regional Standards Committee comments.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports the NPCC Regional Standards Committee comments.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

There is no clear definition of what is a vendor-initiated, remote access and system-to-system remote access. SRP would like to see the definitions clearly defined.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.

Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is Inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
Removing “Interactive” creates ambiguity and negates the need for having a (i) and (ii). The result is (i) remote access, and (ii) system-to-system remote access (which is a subset and included within (i) remote access). Without “Interactive” (ii) is redundant. The resulting requirement then would be, “Coordination of controls for vendor-initiated remote access”. The term “remote access” is unclear and must be further defined. That is why the original language clarified “remote access” using “Interactive Remote Access”(a defined term) and “system-to-system remote access”(commonly understood). Suggestion: define the term “remote access” or put “Interactive Remote Access” and “system-to-system remote access” back into the requirement.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	

Comment
This creates more confusion as CIP-005-7 refers to IRA and vendor remote access. Need to correlate that if the vendor uses IRA, requirements in R2 apply. Correct? Otherwise vendor remote access (system to system) must be through an EAP.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
For the reasons indicated above, GSOC and GTC respectfully reiterates that revisions to strip the requirements down to generic terms like “remote access” and “system to system access” have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms “remote access” and “system to system access” are not defined and, even as modified by the term “vendor-initiated,” could be construed as access from outside an entity’s network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions make clearer the types of remote sessions that are covered by the standards. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	

Comment
MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access. Examples:

- If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement.
- If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access.

Examples:

· If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement.

· If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We recommend that any changes to CIP-005 need to be consistent with changes here.

CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
We believe that the proposed wording changes for R1.2.6 unnecessarily broaden the scope of this requirement. The term "interactive" is key to the wording of this requirement and consistent with the usage of IRA elsewhere in the CIP Standards.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	

Comment
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment
For the reasons indicated above, GTC/GSOC respectfully reiterate that revisions to strip the requirements down to generic terms like “remote access” and “system to system access” have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms “remote access” and “system to system access” are not defined and could be construed as access from outside an entity’s network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: "Coordination of controls for all vendor-initiated remote access." We believe that specifying and breaking down remote access types (e.g. "system to system") adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Without a definition of what System to System remote access is, the changes requested do nothing to clarify anything different that was written in version 2. A definition for system to system remote access needs to be created and added to the Glossary of terms. While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word “initiated” may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). This is evident where established read only sessions between a Registered Entity and the vendor are included as “vendor remote access.” Recommend language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered “access” to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.	
Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the notion that vendor-initiated remote access should be considered. We feel that the standard language needs to address capability versus intent of the remote access. Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions. If a vendor has the capability of implementing changes on a BCS shifts because the vendor is participating in an activity where control of the user's computer could be granted to the vendor (WebEx for example), then this isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what "vendor-initiated" actually is. It would be beneficial to leverage language of Interactive Remote Access such as "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)".	
Likes 0	

Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST does not agree that the desired clarity has been achieved. N&ST recommends simplifying Part 1.2.6 to read: “Coordination of controls for vendor-initiated remote access to applicable systems.”	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	

Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. . We recommend consistency between these Standards and defining terms such as "interactive remote access" and "remote access".	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

We do not agree that the proposed language clearly defines the intended types of vendor remote access.

First, we do not agree that Interactive Remote Access vendor sessions should be treated differently than internal sessions.

Second, Part 1.2.6 (ii) specifies system-to-system remote access but the language is not bound to vendors. The requirement could be interpreted to include all system-system remote access, vendor or internal.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern does not agree with the reconstructed wording. The updated text causes further confusion from the original. During the Webex it was discussed that IRA and system-to-system are sub-sets of vendor remote access. To ensure clarity, Southern would like the SDT to consider the following possible rewording: “Coordination of controls for vendor-initiated (i) Interactive Remote Access, and (ii) system-to-system remote access to BES Cyber Systems. Another requirement for consideration would be to add the following, “1.2.7 Coordination of controls for vendor-initiated remote access (interactive user access and system-to-system access) to applicable EACMS and PACS.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE recommends review of the proposed CIP-005-3 changes to ensure consistency.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	
Comment	

NV Energy supports the notion that vendor-initiated remote access should be considered in CIP-013-2 R1, P1.2.6; however, we feel that the standard language needs to address the capability of the vendor while having access versus the intent of the vendor's remote access.

Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions.

However, there is an ambiguity when it comes to the remote sharing applications between Entity and Vendor (i.e. webEX, Skype, Zoom, etc.), in that during these remote sharing events, a user's (Entity) computer can grant to the vendor control of their screen. NV Energy believes that this event isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.

Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	
Comment	

The use of the word "initiated" may have unintended consequences that defy the security intent. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. ATC requests consideration of alternative language that focuses on the risk itself. Additionally, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). Consequently, established read only sessions between a Registered Entity and the vendor are being lumped into the "vendor remote access" bucket. ATC requests consideration of qualifying language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered "access" to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS

Likes 0	
Dislikes 0	
Response	

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	No

Document Name	
Comment	
While the SDT does a good job in reconstructing the wording, it only addresses “’vendor” and “system-to-system” access. Remote access to BES Cyber Assets and Systems can be granted by the entity to not only its employees, but to its vendors and contractors, separate and outside from access granted to other vendors or systems.	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
It is better to use the defined terms that are used throughout the standards. Using "remote access" instead of "Interactive Remote Access" implies what is being addressed in this requirement different than Interactive Remote Access in ways other than being vendor-initiated. Also, the source of initiation is not clear with system-system remote access, but if a vendor is compromised, any system-to-system remote access with that vendor should be terminated without regard to who initiated it. The original language is better.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: “Coordination of controls for all vendor-initiated remote access.” We believe that specifying and breaking down remote access types (e.g. “system to system”) adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
The changes to CIP-013-2 Part 1.2.6 appear to have had the opposite effect. Now there is no clarity about what a vendor-initiated remote access session is. Does “access” refer to read-only access? Or does “access” only refer to control? What is the meaning of “remote” in this situation? “Remote” to an applicable system? How is that clarified? Additionally, it appears that (ii) system-to-system remote access, is now just a subset of (i) remote access. Tacoma Power does not support these changes to CIP-013 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes “Coordination of controls” remains somewhat ambiguous. Inclusion of “vendor-initiated” for both remote access and system-to-system remote access is somewhat redundant and confusing. BPA proposes the following:

1.2.6. Coordination of remote access controls for vendor personnel or systems accessing BES Cyber Systems ESP/ESZ to include; reasons and requirements for remote access, periodicity of access (temporary or permanent), methods of authentication, and revocation processes for personnel.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 that all types of vendor-initiated remote access need to be considered then the wording used in CIP-005-7 should be consistent with the wording used in CIP-013 R1, Part 1.2.6. In CIP-005 “vendor initiated remote access” is used while both “vendor initiated remote access” and system to system remote access is used in CIP-013 R1, Part 1.2.6.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle City Light concurs with the comments provided by Snohomish PUD

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	No
Document Name	

Comment
Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word “initiated” may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). This is evident where established read-only sessions between a Registered Entity and the vendor are included as “vendor remote access.” Recommend language to exclude established non-persistent read-only sessions (i.e. WebEx) from being considered “access” to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	

Comment
CIP-013-2 R1, Part 1.2.6 requires one or more processes used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access. This language provides the two basic types of vendor remote access; however, it lacks the detail provided in CIP-005-7 R3, Parts 3.1 and 3.2, which may be required to effectively assess risk. Further, as discussed in the previous comments, the use of the term “vendor-initiated” is troubling because it should not matter whether the vendor

or the entity initiates the connection. By considering only vendor-initiated connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree with the changes; we believe the CIP-013-1 language is more clear and comprehensive.

The previous CIP-013-1 wording

• “Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)”

is more clear and more comprehensive than the proposed CIP-013-2 wording

• “Coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access.”

CIP-013-2’s “Coordination of controls for vendor-initiated … system-to-system remote access” seems to exclude system-to-system remote access that’s internally-initiated, where a system inside the ESP automatically creates a remote access session with a vendor’s system in the vendor’s network.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders’ time on this endeavor which will likely change in the near future as a result of DOE’s efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 6

Answer	No
Document Name	

Comment

We recommend that any changes to CIP-005 need to be consistent with changes here.

CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.

Likes 0	
Dislikes 0	

Response

Scott Tomashefsky - Northern California Power Agency - 4

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees with clarifying that all types of vendor-initiated remote access needs to be considered. Texas RE recommends that the term “vendor” be defined in the NERC Glossary. Although it is defined in the Supplemental Material, that material is not part of the standard and is not enforceable. There is still confusion on who and what is a vendor.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) supports the position that all vendor-initiated remote access needs to be considered.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree with this revision that clarifies vendor-initiated remote access controls in supply chain risk management plans and processes.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the reconstructed the wording clarifies that all types of vendor-initiated remote access needs to be considered.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	

Response
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6
Answer	
Document Name	
Comment
I support EEI's comments.
Likes 0	
Dislikes 0	
Response
Neil Shockey - Edison International - Southern California Edison Company - 5
Answer	
Document Name	
Comment
Please see comments submitted by Edison Electric Institute
Likes 0	
Dislikes 0	
Response
Kenya Streeter - Edison International - Southern California Edison Company - 6
Answer	
Document Name	
Comment
Please see comments submitted by Edison Electric Institute
Likes 0	
Dislikes 0	
Response

Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
We think 24 months better supports the process we have at a small utility with minimal IT resources.	
Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Due to the Covid-19 impacts to industry, we suggest considering a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments

Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24-month implementation plan.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

It appears that the basis for the originally proposed 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high impact and medium impact BES Cyber Systems. This supposition would make it appear that it is a straightforward expansion of existing Supply Chain programs to EACMS and PACS. This is not true in all cases. Notably, the high impact (e.g. control center) and medium impact (e.g. substation)

environments are very different. CEHE believes that such a difference justifies a longer implementation period. CEHE suggests that 18 months is not enough and proposes a 24-month implementation plan instead.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
These changes are adjustments to existing standards, and 12 months is plenty of time to implement the changes.	

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

Due to the on-going Covid-19 impacts and delay of initial supply chain standards implementation, it is recommended to consider a 24-month implementation plan.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Due to the development of the virtualization standards, and supply chain standards implementation overall, we recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	No
Document Name	
Comment	
In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.	
Likes 0	

Dislikes 0	
Response	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with a longer implementation plan window.	
Likes 0	
Dislikes 0	
Response	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
We agree with the SDT proposal	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports the 18 month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes

Document Name	
Comment	
NV Energy agrees that the the extension in implementation timeline is acceptable; however, with the expectation of revisions to the CIP Standards through Project 2016-02, and the concurrent work required to implement these future changes, NV Energy would request that NERC look to further extend this implementation timeline to ensure Entities have enough time to implement the concurrent revisions.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) supports the 18-month implementation plan and the extended implementation period appropriate when considering the expanded applicability of the Standards.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes

Document Name	
Comment	
Although 24 months would be more appropriate, GTC/GSOC appreciate the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO agrees with the increase of the implementation period from 12 moths to 18 months. IESO would prefer 24 months to take budget cycles into account. Although the we acknowledges that EACMS and/or PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and or PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Although 24 months would be more appropriate, GSOC and GTC appreciates the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles. Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.	
Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles.

Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.

Likes 0	
Dislikes 0	

Response

Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	

Comment

NO. See response to question 7.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Neil Shockey - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	

Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP would first like to see the definitions that are outlined in CIP-005 and CIP-013 with more clarity and a better definition for each.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is supporting the IRC SRC Comments as follows:

Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO

Answer	No

Document Name	
Comment	
In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
It's difficult to determine the cost since CIP-013 is not effective and no studies have been conducted to determine the cost to implement across the industry. Including PACS and EACMS adds another layer to consider once the BCS' Supply Chain Risk Management requirements are implemented. The scope continues to expand without consideration to the industry as a whole to first achieve the risk mitigations for the initial standards and without studies to determine the effectiveness of the Supply Chain Risk Management standards for BCS'. Unless small entities contract with 3rd parties for the vendor risk assessments required, what is their alternative since vendors usually do not respond to their cyber security	

questionnaires. Suggest determining the effectiveness of the first CIP-013 standards before adding more systems to the requirements and potentially adding additional costs.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

While GSOC and GTC acknowledges the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
While GTC/GSOC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	

Comment
We do not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known. .

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment
The current language in the standard intentionally creates different expectations for vendor remote access versus internal staff remote access. As this subjects the entity to potentially multiple frameworks for the same activity, it inherently creates an inefficiency to the process that could be easily eliminated. Furthermore, the current measures in CIP-005 Part 3.1 introduce process activities that go beyond the stated requirements (i.e. monitoring remote access activity), potentially leading entities to implement more costly approaches to meet the standard requirements.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	

Comment
Although ISO-NE acknowledges that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors to ensure they are implemented in the most cost-effective manner. At that time, the ISO-NE also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
The ambiguity around what "access" is, what "remote" is, and what "vendor" is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Additional costs will be driven to add those new EACMS and PACS assets to supply chain overview.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Depending upon how an entity implements their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they may need to develop and implement a different process for EACMS and PACS systems.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
To minimize churn among standard versions, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-005-7, CIP-010-4, and CIP-013-2 with other existing drafting teams for related standards; specifically, Projects 2016-02, 2020-03, and 2020-04. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.	
Likes 0	

Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	

Comment
Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test, and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost-effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result. Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost-effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020, clearly states the position that “CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements.” For this to be a truly objective-based Standard the requirement language should encourage “reliability and security” such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the “knowns” and effectively mitigate the risk of the “unknowns”. The simple inclusion of something like “1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances”.

Likes 0	
Dislikes 0	

Response
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric
Answer	No
Document Name	
Comment
Inclusion of EACMS and PACS to CIP-005 R3 Part 3.1 will require significant investment to isolate these Boundary Assets to be able to monitor for and terminate vendor remote access sessions. This is a substantial change to definition of EACMS and PACS and likely will bring additional assets into scope by requiring entities to define the new boundaries and cyber security isolation methods that had previously not been required.
Likes 0	
Dislikes 0	
Response
Kjersti Drott - Tri-State G and T Association, Inc. - 1
Answer	No
Document Name	
Comment
Tri-State recommends EACMS be separated into EACS and EAMS. Not separating the concept of an EACMS into an EACS and EAMS creates lower BES security, as monitoring of industrial control system networks is not being integrated with monitoring of business networks, sensor networks, and other networks. A particular pain point is that EACMS requirements prevent outsourcing 24x7 network monitoring that includes systems or networks in CIP scope. The financial and human resources needed to apply EACMS compliance levels to monitoring (not controlling) are unnecessary.
Likes 0	
Dislikes 0	
Response
Dennis Sismaet - Northern California Power Agency - 6
Answer	No
Document Name	
Comment
This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known to establish a baseline with which to measure against.

Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools in the required time period. Also, Duke Energy has yet to evaluate the impacts of defining and implementing EACMS and PACS related controls to meet this requirement.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No

Document Name	
Comment	
We do not feel that the level of administration and additional work is not cost effective for small organizations with limited resources. We recommend that exceptions are made for smaller entities that are more limited in their ability to get competative bids, and services to meet the intent of the FERC directives.	
Likes 0	
Dislikes 0	
Response	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the FERC directives can be executed in a cost-effective manner. There will be an undue cost and burden initially to conduct business another way by adding EACMS and PACS to CIP-005 R3.1 and R3.2. Other costs will include providing new technology if not already present to track, store, and recall the data addressing the assessments provided by CIP vendors.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	

Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL

Answer	
Document Name	

Comment

Evergy (Westar Energy and Kanas City Power & Light Co.) does not have a position nor comments in response to Question 6.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	
Document Name	

Comment

The addition of EACMs and PACs to the CIP-005 requirement 3 adds significant compliance efforts and costs to responsible entities. Entities that use vendors to assist in access monitoring, electronic or physical, for monitoring and threat hunting is a good thing. The more eyes on potential nefarious activity provides for a safer and more reliable grid.

Efforts like this sound good but do nothing to add to the cyber security of the grid.

Using the measure cited in part 3.1 as an example "Methods for monitoring activity (e.g. connection tables or **rule hit counters in a firewall**, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions" are now standard in most firewalls and can be provided as a print out for evidence. This however does nothing to secure the grid. The standards should address alerting on and actions taken on a unrecognized connections by an outside source. This would be more in line with providing cyber security, automated processes that transmit logs to SEIMS monitored by outside vendors is better for security. These types of issues should be addressed in CIP-013 requirement 1 already addresses connections inbound and outbound to assets.

Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result.

Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that “CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements.” For this to be a truly objective based Standard the requirement language should encourage “reliability and security” such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the “knowns” and effectively mitigate the risk of the “unknowns”. The simple inclusion of something like “1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances”.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Linn Oelker - PPL - Louisville Gas and Electric Co. - 6

Answer	
Document Name	

Comment

I support EEI's comments.

Likes 0	
Dislikes 0	

Response

Neil Shockey - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	

Comment

NO. See response to question 7.

Likes 0	
Dislikes 0	

Response

7. Provide any additional comments for the standard drafting team to consider, if desired.

Calvin Wheatley - Wabash Valley Power Association - 1,3	
Answer	
Document Name	

Comment

Wabash Valley Power Alliance supports the comments submitted by NRECA.

We individually comment that the low impact category has highly varied risk levels. This is especially true when a single access point controls access to a large number of BES assets. It is essential to impose BES Reliability standard on those systems whose architecture has a potential broad scale affect on reliability, while not adding excessive burden and costs on systems that are architected to have a minimal effect on grid reliability. Appropriate risk assessment by the SDT to focus efforts on those systems that will have an affect on grid reliability should be included as a component of the SAR.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	

Comment

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending an inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provide a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed though the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent out for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as

the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	
Document Name	
Comment	
AZPS requests more information be provided regarding the rationale for leaving the “system-to-system remote access” and “Interactive Remote Access” language in the Measures section of CIP-005-7 R3.1 and R3.2, after removing the language from the requirements. AZPS notes that the Measures section for CIP-005-7 R3.2 still references disabling remote access versus terminating remote access sessions. AZPS recommends that the SDT revise the Measures to maintain consistency with the requirement language. Similarly, AZPS recommends revising the language in CIP-013-2 R1.2.6 to maintain consistency with the language in CIP-005-7 R3.1 and R3.2.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	

Answer	
Document Name	
Comment	

Within CIP-010-4 Requirement 1 Part 1.6, PCAs should also be included in the Applicable Systems. When BES Cyber Systems and PCAs are located within the same ESP and software is validated and verified for the BCS but not the PCAs, a mixed-trust security environment is created within an ESP.

The CIP-005-7 Implementation Guide for R3 uses the term “periodic” in every example of internal controls – with no definition or assistance regarding how long “periodic” is.

Likes 0	
Dislikes 0	
Response	
Erick Barrios - New York Power Authority - 6	
Answer	
Document Name	
Comment	

Request that NERC notify the industry when posting an update or an additional document after announcing that project’s comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.

In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, “General Considerations for Requirement R2” should read “General Considerations for Requirement R3”. The text indicates “The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls “. R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.

Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders’ time on this endeavor which will likely

change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP STD not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

Support SDT consideration of formally defining "vendor" in the NERC Glossary of Terms. With the supply chain CIP-013-2, suggest inclusion of PACS peripherals (badge readers).

There are significant risks associated with PACS peripherals.

When contactless smart cards are implemented and deployed properly, they represent one of the most secure identification technologies available. However, some manufacturers, in an attempt to sell a 'universal' reader capable of reading almost any contactless smart card technology, actually disable the built-in security mechanisms. These readers, referred to as 'CSN readers', only read the card's serial number which, per ISO standards, is not be protected by any security. The ISO standard specifies use of the CSN for a process referred to as anti-collision, which is designed only to identify more than one distinct card in the field of the reader, and does not include security measures. An understanding of these details can allow a perpetrator to build a device to clone (or simulate) the CSN of a contactless smart card.

CSN refers to the unique card serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443and 15693. The CSN goes by many other names including UID (Unique ID), and CUID (Card Unique ID). It is important to note that the CSN can always be read without any security or authentication per ISO requirements.

Providers who seek to provide the lowest cost product, often choose not to pursue proper licensing of the security algorithms to minimize their costs. They also often fail to educate their customers on the compromise they are introducing into the customer's security solution. While the customer may benefit from a low price at install, the long term cost of a security compromise can be catastrophic. (Source - HID Global)

Emerging PACS technology includes IP Based Door Access and Entry Control Systems. This eliminates the need for a door controller. The built in intelligence system within the badge reader allows the access control decision to be made at the door controller in the event the network is down.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments".

The changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following:

CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors, or vendors).

CIP-002 is a more appropriate choice for identifying and categorizing vendor systems that reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access – much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people).

CIP-005, CIP-007, and CIP-010 already address controls for configurations, accounts, and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case, the justification would be "vendor remote access."

These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
There are cases where the requirements would include “BES Cyber Systems, and their associated EACMS and PACS” as Applicable Systems (such as in CIP-010-4 Part 1.6, CIP-013-2 R1, R1.1, R1.2, R1.2.5). If associated PCAs are not included, the rest of the cyber assets within an Electronic Security Perimeter will be vulnerable. For example, PCA patches may be inadvertently loaded with Trojan Horses, malicious sniffers, etc., which may affect the rest of the devices in the network – including BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	

Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
Santee Cooper has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	
Document Name	
Comment	
Consistency across the three supply chain standards is of paramount importance. Please consider integrating consistent language into each standard, as applicable.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	
Document Name	
Comment	

The clarification of vendor-initiated in CIP-005 R3 is valuable, but it doesn't solve the challenge of a contract employee (a vendor according to Supplemental Material sections of the Standards). A contract employee who initiates access to an applicable system remotely would be subject to these requirements, even if they are using Registered Entity owned and managed systems to initiate that access.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	
Document Name	
Comment	

Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.

In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	
Document Name	

Comment

No additional comments on this question.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5

Answer	
Document Name	

Comment

CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)

CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	

Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	

Comment
The continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that “CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements.” For this to be a truly objective based Standard the requirement language should encourage “reliability and security” such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively plan for the “knowns” while effectively mitigating the risk of the “unknowns” without a violation. The simple inclusion of something like “1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances”. ATC believes it was the original SDT’s intention for this to be a future-looking planning standard instead of a real-time/near real-time operating horizon standard, and does not believe it was the original drafting team’s intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation. If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are “unplanned” and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.

Likes 0	
Dislikes 0	

Response

Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	

Comment
I support EEI's comments.

Likes 0	

Dislikes 0	

Response

Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan

Answer	
Document Name	

Comment

CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)

CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

Southern would like, as with EEI, for the SDT to more clearly define how vendor remote access is to be addressed when a staff augmented contractor is essential to the reliable operations to the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services that include regular access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA.

Consider a proposal to modify the SAR to remove EACMS from the scope of CIP-005.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
We appreciate the SDT efforts. Cyber Security is an ever changing issue and the Standard development process is just too slow for specifics. We believe entities should be required to regularly evaluate the risks and develop their own risk-based mehods of protection. This approach would allow entities to concentrate more on protecting the BES and less on complying with specific requirements that may or may not be adequate or cost effective. This approach would likely result in fewer findings of non-compliance and more recommendations for improvement, but provide more effective Critical Infrastructure Protection.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	
These changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT may must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following: CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors or vendors). CIP-002 is a more appropriate choice for identifying and categorizing vendor systems which reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access –	

much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people).

CIP-005, CIP-007 and CIP-010 already address controls for configurations, accounts and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case the justification would be “vendor remote access.”

These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.

Secondly, the continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that “CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements.” For this to be a truly objective based Standard the requirement language should encourage “reliability and security” such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational.

NERC should implement language to fix this so we can effectively plan for the “knowns” while effectively mitigating the risk of the “unknowns” without a violation. The simple inclusion for example of “1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances”.

It was the original SDT’s intention for this to be a future-looking planning standard team instead of a real-time/near real-time operating horizon standard, and was not NERC nor the original drafting team’s intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation.

If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are “unplanned” and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.

Likes 0	
Dislikes 0	

Response

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez

Answer	
Document Name	

Comment

N/A

Likes 0	

Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	
Request that NERC notifies the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that the industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to	

reassess selected supply chain cybersecurity risk management controls “. R2 requires the responsible entity to implement its supply chain cybersecurity risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	
Document Name	

Comment

EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner’s CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

Request that NERC notify the industry when posting an update or an additional document after announcing that project’s comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.

Likes 0	

Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	

Comment
EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation of the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner's CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	

Comment
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.

Likes 0	
Dislikes 0	

Response
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott
Answer	
Document Name	
Comment
ITC is Abstaining
Likes 0	
Dislikes 0	
Response
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3
Answer	
Document Name	
Comment
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.
Likes 0	
Dislikes 0	
Response
Andrea Barclay - Georgia System Operations Corporation - 4
Answer	
Document Name	
Comment
GSOC and GTC notes that the replacement of the term “determine” with the term “detect” in CIP-005-7, R2.4 (now 3.1) creates significant technical issues and may be infeasible. More specifically, the revision to the term “detect” pre-supposes a technical method to automatically delineate or differentiate vendor–initiated sessions from other active remote access sessions, which may be technically infeasible. In the previous version of the Guidelines and Technical Basis, a method to identify all types of remote access and an ability to terminate vendor sessions was considered appropriate. This distinction is important because methods for identifying active remote access sessions may be able to identify active sessions, but may not be able to differentiate those sessions that are vendor-initiated. Accordingly, once active sessions are identified, human or manual intervention

may be necessary to hone in on those sessions that are vendor-initiated, e.g., through use of dedicated vendor identification numbers or access names. For these reasons, GSOC and GTC recommends that the SDT revert the proposed revisions to use the term “determine.”

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

CPS Energy appreciates the standards drafting team efforts and supports mitigating risks to the BES in a cost effective manner across industry.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

We would like to thank the SDT for allowing us to comment on the proposed changes.

Likes 0	
Dislikes 0	

Response

Jose Avendano Mora - Edison International - Southern California Edison Company - 1

Answer	
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2 (Draft 2)
Comment Period Start Date:	5/7/2020
Comment Period End Date:	6/22/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 2 ST

There were 75 sets of responses, including comments from approximately 183 different people from approximately 124 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

6. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. Provide any additional comments for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	Bobbi Welch	MISO	2	RF
					Ali Miremadi	CAISO	2	WECC
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	3		NIPSCO	Joe O'Brien	NiSource - Northern Indiana Public Service Co.	6	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Steve Toosevich	NiSource - Northern Indiana Public Service Co.	1	RF
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Public Utility District No. 1 of Chelan County	Ginette Lacasse	1	WECC	PUD #1 Chelan	Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
					Ginette Lacasse	public Utility Distric No 1 of Chelan	1	WECC
Snohomish County PUD No. 1	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1 of Snohomish County	4	WECC
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Alyssia Rhoads	Public Utility District No. 1 of	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Snohomish County		
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Scott Brame	North Carolina EMC	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Meredith Dempsey	Brazos Electric Power	1,5	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					John Pearson	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Edison Co. of New York		
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Jim Grant	NY-ISO	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					John Hasting	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Lower Colorado River Authority	Teresa Cantwell	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated. Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R2 states "For all Interactive Remote Access, utilize an Intermediate System". However, by creating a new requirement specifically for vendor access there could be confusion that the access is "vendor" related access and R2 is not applicable. Based on the wording of this Question as context, it appears that it's the intent of the SDT to remove intermediate systems for vendor initiated IRA. Thus explicitly allowing direct vendor access to assets in the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. CIP-005-7 R2 Part 2.1 is also silent to the initiator of the access, and therefore IRA is one type of vendor remote access in the context of the BCS and its associated PCAs, and pursuant to CIP-005-7 R2 Part 2.1 the use of an Intermediate System is required. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for remote access to EACMS and PACS specifically. The changes made to CIP-005-7 R3 to apply only to EACMS and PACS should clarify the concern.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No

Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	
Response	

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State recommends that CIP-005-7 R3 plane definitions be expanded, as they are brief and there is no further explanation of the planes in the Implementation Guidance or Technical Rationale. Suggest definitions similar to Cisco examples below:

1) Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network. 2) Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic. End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT will consider your suggested language for the Implementation Guidance or Technical Rationale.	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
The measures include as examples the usage of an EAP or Intermediate System to disable access. By the very nature of the devices, PACS and EACMS are outside of network boundary inclusion for CIP. To now require that termination of vendor access for EACMS and PACS by definition and available technology have required that controls be placed on these devices that contain assets outside of NERC CIP scope. EACMS and PACS should not be included in scope for Supply Chain management until or unless they are required to be placed behind a Firewall and required access via an Intermediate Server. The not do so leaves entities exposed to a wide interpretation during audit on what is an “acceptable” method for identification and termination of vendor access.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. To require an Intermediate System for access into the EACMS would be recursive. The SDT was mindful not to create a 'hall of mirrors'. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. LaGrange has been added to CIP-005-7 R3 Part 3.1 to clarify what is required. That having been said, these requirements do not preclude and entity from going above and beyond the minimums of the Standards to implement a defense in depth approach with additional layers of security.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments The changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard requires an Intermediate System to access an EACMS; and because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS. The entity must implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating another upstream device that qualifies as an EACMS by definition. Recommend language to clarify the term access. This could be "authenticated access, access session, etc..." so it is clear that "a knock on the front door" of the EACMS that authenticates the system/user is NOT considered "access" (or in this case, by extension, "vendor remote access") to an EACMS. This would preclude auditors from interpreting a "knock at the front door of the EACMS that is later denied within the EACMS" as "access to" an EACMS.

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access". Another consideration is to revise CIP-002 to allow entities to define only those systems they use as Intermediate Systems and/or Remote Access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered MRO NSRF's suggestion to add clarifying language to the term "access", to help assure the perceived 'hall of mirrors' issue is resolved. The use of an Intermediate System for EACMS is not required. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1. The SDT added clarifying language to CIP-005-7 R3 Part 3.1 to remove concerns with "knock at the front door" issues. The SDT has considered MRO NSRF's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective. Modifications to CIP-002 are out of scope of the 2019-03 SAR.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1, which requires the use of Intermediate Systems	

for all interactive remote access sessions regardless of the source of initiation. In addition, the definition of EACMS currently includes Intermediate Systems. Based on these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. Additionally, Dominion Energy continues to opine that EACMS should be excluded from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications included in this draft, has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

Dominion Energy is also of the opinion that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because sSystems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

Dominion Energy is of the opinion that the SDT should consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends revising the language of CIP-005-7 R2 Part 2.1 to account for the addition of R3. It is not clear if Part 2.1 carries over and applies to R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intends for CIP-005-7 R2 Part 2.1 to apply for high and medium impact BES Cyber Systems and their associated PCAs, as well as for medium impact BES Cyber Systems with external routable connectivity and their associated BCAs as it relates to vendor remote access. The SDT does not intend for CIP-005-7 R2 Part 2.1 to apply to vendor remote access for EACMS nor PACS. The use of an Intermediate System for EACMS and PACS is not required in the current CIP-005-6 Standard regardless of whether the access is from a vendor or other remote source. Increasing the scope of Intermediate System use to EACMS and PACS is not in scope of the 2019-03 SAR nor is it a directive in the FERC order, therefor, the SDT has made modifications to assure the scope of Intermediate System use is not increased.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to Snohomish PUD.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Moving the language to the new R3 requirement does not make it clearer that Intermediate systems are not required for R3. If this is the SDT's intent, then it should directly state it in the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA notes that the proposed language still cites applicability to EACMS; Intermediate Systems are included in the definition of EACMS so the language still appears to include a requirement to determine active sessions to an Intermediate System, even if the remote session does not continue on the provide access to an asset in the ESP. In addition, not all EACMS are the same; this term has become too inclusive of many different types of technology to apply requirements.

BPA believes the crux of the problem, as demonstrated by previous comments and unofficial ballot responses by multiple entities, is this: The EACMS definition is concurrently being modified by the 2016-02 project and keeping the current definition inclusive of logging and monitoring systems is problematic for the same reasons in both drafting efforts. The level of threat to and risk from a system that 'controls access' vs a system that provides a support function by 'logging or monitoring access and access attempts' is different. Logging and monitoring systems benefit from global oversight and gathering logs from the entire enterprise. Access granting systems benefit from specificity and narrow focus on the asset they are protecting. The CIP standards **must not** discourage or penalize efforts on the part of an entity to modernize their SIEM and threat analysis capability. Adding compliance burden to their enterprise logging and monitoring systems is such a discouragement.

From a standards standpoint, this is not a common approach to address access control and access monitoring, as they are mutually exclusive. Even FISMA breaks them apart as control families as Access Control (AC) and Audit and Accountability (AU) to address access control and access monitoring respectively, as an example.

An example of more precise language (and BPA suggests this for inclusion in Guidelines and Technical Basis) might be:

R3.1 Have one or more methods for DETECTING active sessions (including both system-to-system and Interactive Remote Access, regardless of the identity of the person initiating the session) that traverse an EAP to logically access any applicable cyber asset in the ESP or ESZ.

R3.2 Have one or more method(s) to TERMINATE active sessions as referred to in R3.1

R3.3 Have one or more method(s) to DISABLE INITIATION OF NEW remote access sessions as referred to in R3.1.

Please note the terminology and conceptual change to a 3 part requirement: "Detect/Terminate/Disable". The word "Determine" is unusual usage and not aligned with typical cyber security terminology. The reason for a separate requirement in our proposed R3.3 is simple; terminating existing sessions does not prevent an attacker from spawning new sessions, and it is very easy to automate such requests. The requirement to "disable active vendor remote access" is crippled by the word "active" because it does not clearly express a

need to disable future sessions which are by definition not "active". Combining the two requirements is parsimonious of words to the point of obscuring the objective. Without a means of denying new sessions, whether granularly or globally, an entity could find themselves playing "whack-a-mole" with an adversary and never able to manually keep it with automated requests. An example of granular control might be disabling a specific vendor's remote access account, blocking requests from a specific IP address or range, or changing an authentication token or password for a particular user account's remote access. This could be an absolute block or a suspension on new sessions for a timed period. For a global option, examples include simply denying all remote access attempts via change to a global VPN policy, firewall rule, etc. This is the proverbial "take a fire axe to the Internet connection" option.

The measures column for CIP-005=07 R3.1 includes *"Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access."* While this may be an effective measure for requiring authorization for a remote session, this is not an effective measure for determining an active session, sans a requirement to periodically/automatically terminate active sessions.

The measures column for R3.2 better captures the concept that the remote access to the Intermediate System or other EACMS is not the issue; simply getting a login prompt to a cyber-asset outside the ESP is low risk. Another means of clarifying the risk around Intermediate Systems might be to add Intermediate System to the applicability column to apply the R3.1 requirement to have a detective control, and leave it out of the R3.2(/R3.3 if adopted) applicability column, not requiring a specific ability to terminate/deny sessions to Intermediate Systems, but rather into the ESP/ESZ.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees that a login prompt on an EACMS does not constitute access. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The Electronic Access Control or Monitoring (EACMS) definition is used pervasively within the CIP Standards and it is out of the SDT scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). For

this reason, the SDT has not modified the EACMS definition. Additionally, the 2019-03 team has worked with the 2016-02 team to ensure continuity of changes, at this time both teams assert the change of the EACMS definition is outside of each team's respective SARs. The SDT thanks BPA for offering adjusted language and, as requested, is considering those suggestions for the IG or TR (formerly know and GTB). Furthermore, the SDT has considered comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap of reestablished sessions, to assure the spawing of new sessions is addressed, and to add the necessary flexibility for an entity to determine how to meet the security objective.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
Tacoma Power thanks the SDT for considering our previous comments. Unfortunately, moving the language to a new requirement does not clarify the situation. Our concern is that the typical device used to detect a vendor remote access session is the EACMS that the vendor is accessing. Applying this requirement to an EACMS appears to be requiring an EACMS for an EACMS, producing a hall of mirrors. Additionally, the term "active" has been removed from the language, removing this requirement's role in support of the Part 3.2 requirement, since there is no time-bound nature to the current Part 3.1 language. We could have a method to detect after-the-fact vendor-initiated access, which would serve the Part 3.1 requirement language, but not the needs of Part 3.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of	

EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has considered comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the removal of the word 'active', and to add the necessary flexibility for an entity to determine how to meet the security objective such that the interests of both Parts 3.1 and 3.2 are served.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
If intent is to specifically denote that intermediate systems are not required or in scope, suggest stating so directly: “Intermediate are not required for R3”.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated.	

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Oncor supports the comments submitted by EEI. In addition, without including the language that "Intermediate Systems are not required", it is left to interpretation by the entity. In CIP-005-6, R2.1 and 2.2, use of an Intermediate System is clearly defined.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for our comment, please see the response to EEI comments.	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to Tacoma Power.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC thanks the SDT for attempting to resolve this concern, and agrees with the approach to separate this requirement out into R3; However, unfortunately the hall of mirrors condition still exists with EACMS in the applicability column due to a broader issue of ambiguity in the word "access". Where getting "to" an EACMS associated with a high or medium impact BES Cyber System is considered "access" (or in this case, by extension, "vendor remote access") the entity must still implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating 1) another upstream device that qualifies as an EACMS by definition, 2) a hall of mirrors, and 3) an impossibility of compliance. ATC requests consideration of qualifying language that includes "authenticated access", or something of the like, as the target instead of the ambiguous term "access" so it is clear that "a knock on the front door" of the EACMS that authenticates the system/user is NOT considered "access" (or in this case, by extension, "vendor remote access") to an EACMS. This resolves the hall of mirrors issue and provides necessary specificity to preclude auditors from interpreting a "knock at the front door of the EACMS that is later denied within the EACMS" as "access to" an EACMS.	

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS is not required. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The SDT has considered ATC's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment	
NV Energy supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The proposed changes dated 05/14/2020 do not provide clarity regarding the applicability of CIP-005 R2, which includes the need for an Intermediate System for **all** Interactive Remote Access Sessions. The requirement language does not distinguish between vendors vs. non-vendors; therefore, Intermediate Systems would be required for vendor Interactive Remote Access sessions. Additionally, the current definition for Interactive Remote Access (IRA) in the NERC Glossary of Terms implies R1 and R2 may still be applicable to the new R3. ISO-NE recommends that the SDT incorporate the new IRA definition proposed by the Virtualization SDT in Project 2016-02 Modifications to CIP Standards into this project. ISO-NE also recommends that the SDT return the language that was moved to the new R3 back to CIP-005 R2.4 and R2.5 in order to maintain continuity with the other CIP-005 R2 remote access requirement parts.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required. The Interactive Remote Access (IRA) definition is used pervasively within the CIP Standards and it is out of scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). Additionally, the 2016-02 has a specific directive in their SAR to address the NERC V5-TAG issues, for which IRA is one. For these reasons the SDT has not modified the IRA definition.	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to Tacoma Power.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No

Document Name	
Comment	

Southern does not agree that the new R3 makes it clearer that Intermediate Systems are not required. In CIP-005 R2 Part 2.1, Intermediate Systems are required for ALL Interactive Remote Access sessions regardless of who initiates them. If the intent of this question is about clarity that terminating established vendor-initiated remote access sessions *to an Intermediate System* is no longer required, the answer is no. EACMS is in the Applicability column and the definition of EACMS is "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. **This includes Intermediate Systems.**" By the definition of EACMS, Intermediate Systems are still included in R3.

The proposed requirement would still require the ability to terminate vendor-initiated remote access sessions to the systems most often used to determine whether the session is vendor-initiated or not. Since the undefined term "vendor remote access" we believe includes both IRA and system-to-system access per the currently approved standard, it appears we would be required to determine the identity of the person BEFORE we allow their system to establish a session with our Intermediate System, which is not possible. The vendor's system must establish a session with the Intermediate System in order to even send the user credentials, which are then checked with usually yet another EACMS (such as a domain controller) in order to determine they are a vendor. At that point, the vendor's system has already had access to our EACMS.

We are also concerned about what "remote" means in context of an EACMS such as an Intermediate System. The definition of Intermediate System states it must NOT be located inside an ESP. The Intermediate System is already remote according to most definitions of remote ('outside the ESP') so what is remote to a remote system?

Southern believes for these reasons that EACMS should either not be in the scope of these particular CIP-005 requirements and the security objective is to be able to determine and disable vendor remote access sessions to BES Cyber Systems *by using EACMS to do so*. If there is some other vendor EACMS access that is intended, it should be precisely described and used within a separate requirement from the main objective of protecting the BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The SDT agrees that by definition an Intermediate System is an EACMS, and therefore also agree that an Intermediate System is in scope for the proposed protections where that Intermediate System is the target (or endpoint) of the vendor's remote access. This does not suggest that the Intermediate System must be used for vendor remote access to an EACMS. Instead it means that if an entity has outsourced some function for that Intermediate System to a vendor, and that vendor is compromised, the entity must be able to detect the vendor's established connections 'into' the Intermediate system and take action to remove that vendor's ability to retain that connection (or re-initiate subsequent connections). This vendor remote access 'into' the Intermediate System (EACMS) could be human interaction or machine to machine. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a connection that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a connection that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The SDT added clarifying language in the Requirement 3, Parts 3.1 and 3.2.

The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the “supply chain risk management Reliability Standards” is a term that collectively refers to CIP-013-1; CIP-005-6 R2.4 and R2.5; CIP-010-3 R1.6. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Requirements, unless specifically excluded by the directive. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

“Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments).”

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" For additional clarity, the focus is not limited to vendor remote access through an EACMS into a BCS. The focus also includes vendor remote access into the EACMS or PACS itself, which could ultimately lead to further unauthorized access to the BCS. Otherwise stated with EACMS as the use case, if an entity allows a vendor's untrusted (or less-trusted) system or personnel to remotely connect machine-to-machine or user-to-machine into the entity's EACMS, and the vendor's system is compromised, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely into the entity's EACMS. The security objective is remove a vendor's ability to retain or reestablish remote access sessions for each of these discrete Cyber Systems: - high impact BES Cyber Systems; - EACMS associated to high impact BES Cyber Systems; - PACS associated to high impact BES Cyber Systems; - medium impact BES Cyber System with External Routable Connectivity; - EACMS associated to medium impact BES Cyber System with External Routable Connectivity; and - PACS associated to medium impact BES Cyber System with External Routable Connectivity."

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

We do not believe this requirement is clear with respect to Intermediate Systems. For any Interactive Remote Access, an Intermediate System should be required, no matter the source (vendor vs. internal).

Second, the second bullet in the measures for Part 3.1 discusses monitoring remote activity, which is inconsistent and exceeds the requirement to detect remote access sessions.

Third, the third bullet in the measures for Part 3.1 needs to better explain the methodology the SDT is intending to describe.

Lastly, the SDT is making an arbitrary distinction for vendor remote access that is unnecessary. All remote access (vendor or internal) should be similarly treated in terms of detecting and termination. However, as discussed previously, the expectation for monitoring is not part of the identified requirements and should be removed from the measures.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. To require an Intermediate System for access into the EACMS would be recursive. The SDT was mindful not to create a 'hall of mirrors'. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. That having been said, these requirements do not preclude and entity from going above and beyond the minimums of the Standards to implement a defense in depth approach with additional layers of security. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

We appreciate the SDT efforts. However, this does seem to create a "hall of mirrors" as pointed put by a number of commenters by requiring an intermediate system for an intermediate system. There should also be allowance for CIP exceptional circumstances in CIP-013.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the “interactive remote access” definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project.

More confusion from the “hall of mirrors” – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures

For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

In addition, the CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Vendor remote access is part of remote access. It is not clear why these are separated.	

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the NPPC RSC comments. Please see the SDT's response to RSC NPPC's comments.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST does not agree that the desired clarity has been achieved, especially since for certain types of "vendor remote access," (e.g., Interactive Remote Access to applicable BES Cyber Systems), Intermediate Systems ARE required. Likewise, for user-initiated remote access, vendor or otherwise, to EACMS and PACS systems that happen to be within Electronic Security Perimeters (not altogether uncommon), Intermediate Systems ARE required. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of "vendor remote access" that require Intermediate Systems and types of "vendor remote access that do not, as CIP-005 is currently written, require Intermediate Systems:

Intermediate System required: Vendor remote access that meets the current NERC definition of "Interactive Remote Access" and is therefore subject to CIP-005 R2.

Intermediate System not required: Vendor remote access that does not meet the current NERC definition of "Interactive Remote Access." This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable.

One way to address this might be to break R3 part 3.1 into two sub-parts:

Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2).

Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.

Likes 0	
Dislikes 0	

Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The proposed draft does not exclude the use of an Intermediate System for IRA into EACMS or PACS that are logically located within an ESP because those EACMS would by definition be dual classified as Protected Cyber Assets (PCAs) and therefore subject to CIP-005-7 R2 Part 2.1 based on the inclusion of 'associated PCAs' within the Applicable Systems. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. The SDT appreciates that N&ST has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No

Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
The changes which move Vendor Remote Access remote access from Parts 2.4 and 2.5 to Parts 3.1 and 3.2 better clarify the requirements for entities, however adding EACMS to the scope of the standard begs the question if an entity now needs another EACMS Intermediate System to access an EACMS? Because an Intermediate System is already defined as an EACMS (because it provides electronic access), and hence the change requires an entity to deploy a separate Intermediate (EACMS) to access the Intermediate System that provides access to the BCS. The entity must implement another upstream control beyond that EACMS in order to disable the access "to" it, thereby creating another upstream device that qualifies as an EACMS by definition. Personnel (employees, vendors, suppliers, contractors, etc..) need to be defined in CIP-004. Systems (vendor or entity owned and maintained) need to occur in CIP-002. Why not revise CIP-002 and allow entities to define only those systems they use as Intermediate Systems and/or Remote Access? Or vendor systems? Why not revise CIP-004 to address vendors?	

Additionally, Requirement R3 Part 3.2 is a "how" in disguise instead of an objective "what". Another potential solution to consider could be the following: Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability to for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating established sessions alone may not preclude the re-establishment of another session). This language could also resolve the hall of mirrors because now the entity can define the revocation point that precludes authentication and subsequent use within the layers of EACMS controls, and the "knock at the front door" to the EACMS is no longer "access".

Secondly, the standard does not clearly define what System to System remote access is. A valid definition for system to system remote access needs to be created and added to the Glossary of Terms.

Lastly, Requirement 3 also conflicts with Requirement 1 part 1.3. If a Responsible Entity (RE) determines that a connection to a vendor is needed and has placed the appropriate controls on the appropriate interfaces of its protecting asset(s) (Firewalls, routers, etc..) then the connection is needed. Secondly the RE is responsible for determining if a vendor has adequate security controls in place or has applied mitigations as part of their CIP-013 process for that vendor then the requirement 3 is not needed. Connections made from a vendor (type, duration and need) should be spelled out in the procurement contracts derived out of the CIP-013 processes.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS is not required. The SDT intention is to be clear that an Intermediate System is not required for remote access to EACMS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

Modifications to CIP-002 and CIP-004 are out of scope of the 2019-03 SAR.

The SDT has considered WAPA's comments to modify CIP-005-7 Requirement R3 Part 3.2 as more objective level language to shore up the perceived gap from the use of the word 'terminate', and to add the necessary flexibility for an entity to determine how to meet the security objective.	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	No
Document Name	
Comment	
If intent is to specifically denote that the intermediate systems are not required or in scope it should be specifically stated "Intermediate systems are not required for R3"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The removal of the term “interactive” and the retention of the terms “remote access” alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term “remote access” is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. For this reason, GTC/GSOC do not agree that the proposed revisions makes it clearer that Intermediate Systems are not required. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
In our opinion the original language in CIP-005-6 stating vendor remote access as system-to-system and interactive is clear and encompassing of all vendor remote access. No change is required to further clarify use of an Intermediate System. However, if further clarification that an Intermediate System is not required I propose the following: "Have one or more methods for determining active vendor remote access sessions (including system-to-system remote access, vendor initiated system-to-system remote access with or without use of an Intermediate System as well as Interactive Remote Access)."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT has considered these suggestions and added clarifying language to CIP-005-7 Requirement R3.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.

Likes 0	
Dislikes 0	

Response
The SDT thanks your for your comments, please see response to EEI Comments.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment
Vendor remote access is part of remote access. It is not clear why these are separated.

Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition of change needs to happen as part of this project. More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors. Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established of union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base. The Interactive Remote Access (IRA) definition is used pervasively within the CIP Standards and it is out of the SDT scope of the 2019-03 SAR to modify NERC Glossary of Terms definitions that impact CIP Standards outside those that are considered the supply chain risk management Reliability Standards; CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). Additionally, the 2016-02 has a specific directive in their SAR to address the NERC V5-TAG issues, for which IRA is one. For these reasons the SDT has not modified the IRA definition. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate

System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO, in general, supports the comments submitted by NPCC and by IRC The wording of Requirement R3 suggests that these are only requirements that apply to vendor initiated remote access and may miss the embedded requirement in Requirement R2. IESO recommends that the wording of Requirement R2 should explicitly add “including vendor initiated interactive remote access” as reminder that there are additional requirements for vendor initiated remote access outside of Requirement R3	

While it is preferred, from a cyber-security perspective, to utilize an intermediate system for vendor initiated interactive remote access to EACMS and PACS, IESO recognizes that it may not be appropriate in all situations	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to NPPC RSC's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI does not agree that the modifications made to the second draft of CIP-005-7, Requirement R3 clarify that Intermediate Systems are not required. This modification conflicts with Requirement R2, subpart 2.1; which requires the use of Intermediate Systems for all interactive remote access sessions regardless of the source of initiation. Also, the definition of EACMS includes Intermediate Systems. For these reasons, Intermediate Systems cannot be excluded. Moreover, Requirement R3 makes EACMS applicable to this requirement. EEI additionally notes that our comments to the previous draft suggested excluding EACMS from the applicability section of Requirement R2, subpart 2.5. Moving this requirement, along with the minor modifications has not solved the issues identified in our comments to the earlier draft of CIP-005-7.

It is our understanding that "vendor remote access" includes both Interactive Remote Access (IRA) as well as system-to-system access. Consequently, entities would be required to determine the identity of the source of communications before they can establish a session with the Intermediate System, which is not possible because systems must establish a session with the Intermediate System in order to receive user credentials, which are then generally checked with another EACMS (such as a domain controller) in order to determine whether the source is a vendor. At this point, the vendor's system has already had access to the entity's EACMS.

For these reasons, we ask the SDT to consider removing EACMS from the scope of CIP-005 Requirement R3. We understand that the security objective for this requirement is to determine and disable vendor remote access sessions to BES Cyber Systems by using EACMS. If this is incorrect, we ask the SDT to more clearly described the objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. The focus is not limited to vendor remote access through an EACMS into a BCS. The focus also includes vendor remote access into the EACMS or PACS itself, which could ultimately lead to further unauthorized access to the BCS. Otherwise stated with EACMS as the use case, if an entity allows a vendor's untrusted (or less-trusted) system or personnel to remotely connect machine-to-machine or user-to-machine into the entity's EACMS, and the vendor's system is compromised, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely into the entity's EACMS. The security objective is remove a vendor's ability to retain or reestablish remote access sessions for each of these discrete Cyber Systems: - high impact BES Cyber Systems; - EACMS associated to high impact BES Cyber Systems; - PACS associated to high impact BES Cyber Systems; - medium impact BES Cyber System with External Routable Connectivity; - EACMS associated to medium impact BES Cyber System with External Routable Connectivity; and - PACS associated to medium impact BES Cyber System with External Routable Connectivity.	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Andrea Barclay - Georgia System Operations Corporation – 4	
Answer	No
Document Name	

Comment
The removal of the term "interactive" and the retention of the term "remote access" (now, undefined) alone do not clearly eliminate the ambiguity regarding intermediate systems. In fact, because the term "remote access" is undefined, the modifications have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply as discussed below in GSOC's and GTC comments in response to Question 2. For this reason, GSOC and GTC does not agree that the proposed revisions make it clearer that Intermediate Systems are not required. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required. The NERC – Cyber Security Supply Chain Risks, Chapter 2 recommended the 2019-03 SDT to develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. The SDT considered this recommendation and proposes the modified language in CIP-005-7 Requirement R3 to include PACS as an Applicable System. The SDT affirms its previous response to previous comments and has incorporated this into the Technical Rationale. That response is as follows: The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",

2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The NERC definition of Electronic Access Control or Monitoring Systems clearly states that Intermediate Systems are also considered as EACMS. Recommend specific language to address "Electronic Access Point(s)" for system to system remote access and intermediate systems for vendor IRA. It is inferred, however, not clear, that an Intermediate system is not required for system to system access, but is needed for IRA. Separating the two parts into another requirement would make it clearer, however in R2.1 the requirement still reads that for **all** Interactive Remote Access, utilize an intermediate system. Somehow it still creates confusion if it's required for "all" but not for vendors? In Requirement R2, Part 2.1, revise "all" remote sessions must be through an Intermediate System and add "excluding vendor system to system remote access through an EAP." Additionally, the requirement R3 Part 3.1 states "to detect" vendor-initiated remote access sessions. In the Examples of evidence, "Methods for accessing logged or monitoring information…" implies that the Responsible Entity is required to monitor vendor activity during the remote session. Is the objective to detect or to monitor the vendor remote access session or both? For instance, once the vendor remote session is detected or established, is the Responsible Entity required to monitor the vendor activity continuously during the remote session or just receive periodic alerts that the session remains open with the ability to terminate as needed?	

Likes 0	
Dislikes 0	

Response

Thank you for your comments. An Intermediate System is not required for system to system access, but is required for IRA where the Applicable Systems indicates it is required. The word "all" in CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs, and here an Intermediate System is required for IRA. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. The SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS is not required.

The objective is for the entity to have methods to detect vendor remote access sessions such that if a vendor's system is compromised, and that vendor's untrusted (or less-trusted) system or personnel are (or can) remotely connect machine-to-machine or user-to-machine into the entity's Applicable Systems as cited in each Requirement Part within R3, then that entity must make sure the vendor's compromised system and personnel are no longer connected remotely (or able to reconnect remotely) into the entity's Applicable Systems. Depending on the Requirement Part, this includes 1) remote access by a vendor into the EACMS or PACS; 2) remote access by a vendor that goes through an EACMS into a high impact BES Cyber System and its associated PCAs; and remote access by a vendor that goes through an EACMS into a medium impact BES Cyber System with External Routability and its associated PCAs.

EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS.

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020

Answer	No
Document Name	

Comment
The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP includes Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter. For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside of the ESP as the proposed language introduces an unsolvable problem. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.
Likes 0
Dislikes 0
Response
Thank you for your comments. There is no intention, nor implied requirement, for EACMS or PACS to holistically inherit all requirements for BES Cyber Systems, nor is there any requirement to for entities to rearchitect their environment to include EACMS or PACS within an ESP. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and

Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within CIP-005-7.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The purpose of CIP-005 is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP). The ISO/RTO Council Standards Review Committee (IRC SRC) is supportive of adding PCAs to CIP-005 since PCAs are already defined as a Cyber Asset within an ESP, but EACMS and PACS are not part of the ESP. The concern is that extending the scope of CIP-005 to include EACMS and PACS will require EACMS and PACS to be treated as if they are part of the network inside of the ESP. By definition, Cyber Assets that perform electronic access control or electronic access monitoring of the ESP include Intermediate Systems and according to the Intermediate Systems definition, an Intermediate System must not be located inside the Electronic Security Perimeter. For these reasons, the IRC SRC is against adding EACMS and PACS for the added scope of network inside the ESP as the proposed language introduces an unsolvable problem. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Finally, the IRC SRC believes it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. There is no intention, nor implied requirement, for EACMS or PACS to holistically inherit all requirements for BES Cyber Systems, nor is there any requirement to for entities to rearchitect their environment to include EACMS or PACS within an	

ESP. The Applicable Systems in a given Requirement Part are mutually exclusive of that of another Requirement Part, and the presence of EACMS and PACS in Parts within R3 neither not supersede nor modify the scope of the Applicable Systems in any other Requirement Part. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within CIP-005-7.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
R2.1 states that an Intermediate System is required for all IRA. Vendor access is not excluded. Moving vendor access from Part 2 to Part 3 does not change that R2.1 is required. SRP recommends language in the standards are made clearer to indicate Intermediate Systems are not required in R3	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. The SDT has elected to keep EACMS and PACS out of Requirement R2 Part 2.1 to prevent confusion of the 'hall of mirrors' and believes the consistency gained by reintroducing EACMS and	

PACS to Requirement R2 Part 2.1 would not be worth the ambiguity it breeds. For these reasons, SDT added clarifying language in CIP-005-7 R3 to bring further clarity that an Intermediate System for vendor remote access into an EACMS or PACS is not required.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to NPPC RSC's comments.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes

Document Name	
Comment	
Duke Energy agrees that the proposed modifications in CIP-005-7 makes it clearer that Intermediate Systems are not required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to move all Vendor Remote Access requirement remote access from Parts 2.4 & 2.5 to Parts 3.1 and 3.2 since it is clearer that Intermediate System is not required for Interactive Remote access to EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
The addition of the Applicable Systems to the Requirement Parts (by itself) makes it clear that Intermediate Systems are not required for vendor remote access; some of these applicable systems cannot reside in a defined Electronic Security Perimeter. The term "vendor-initiated" is troubling because it should not matter whether the vendor or the entity initiates the connection; the risks are identical either way. By specifying only "vendor-initiated" connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement. WECC recommends removing the term "vendor-initiated" to ensure risks of vendor access connections are addressed, whether vendor or entity initiated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intention is to be clear that an Intermediate System is not required for Interactive Remote Access to EACMS and PACS. Intermediate Systems are required for IRA into the high impact BES Cyber System and its associated PCAs, as well as the medium impact BES Cyber System with External Routable Connectivity and its associated PCAs, including vendor remote access. The SDT has considered concerns about the use of "vendor-initiated" and recognizes that risks may be higher when access is initiated from vendor equipment vs. access initiated from entity owned equipment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While this does make it clearer, as a part of the standard's Supplemental Material this should be spelled out, so there is no gray area.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT will revisit supporting material and include clarifying content.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	

Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 7 for Northern California Power Agency	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees an additional Intermediate System is not needed for access to an EACMS Intermediate System, and that the SDT's addition of a new Requirement R3 clarifies this fact. Texas RE notes that, as presently drafted, the proposed Requirement R3 does not require multi-factor authentication and encryption for PACS and EACMS. Vendor remote access brings an increased risk of threats and vulnerabilities to registered entities' CIP environments. For example, a malicious actor could gain access to and/or control of the EACMS and PACS for multiple registered entities through a single compromised vendor. Requiring multi-factor authentication and encryption controls would help decrease the risk of misuse, compromise, and data breach through vendor remote access sessions. As such, Texas RE suggests that the SDT consider incorporating multi-factor authentication and encryption requirements into the proposed Requirement R3. Alternatively, the SDT could implement these requirements by adding PACS and EACMS to the Applicable Systems subject to Requirement R2, Parts 2.1 – 2.3, while retaining the proposed Parts 2.4 and 2.5 from Draft One and incorporating clarifying language explaining that when an Intermediate System is an EACMS, another Intermediate System is not required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT intentionally moved EACMS out of CIP-005-7 R2 in response to significant industry concern regarding the hall of mirrors. EACMS is a term that is pervasively used throughout the CIP Standards, and while the FERC Order directs the SDT to increase the scope of vendor remote access detection, monitoring, and response actions for EACMS, requiring multi-factor authentication and encryption requirements globally for EACMS and PACS may be outside the scope of the 2019-03 SAR and a change the SDT cannot make. The SDT acknowledges Texas REs risk concerns.	

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. NPCC RSC did not provide comments for Question 2.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is no definitive definition of what is an active vendor remote access session including system-to-system remote access as well as Interactive Remote Access, which includes vendor-initiated sessions. SRP would like to see clear definitions added to the Glossary of Terms and examples of each within the Guidelines and Technical Basis.	
Likes 0	

Dislikes 0	

Response
Thank you for your comments. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR (formerly known as GTB) to bring further clarity.

Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	

Comment
CIP-005, R3.1 “Detecting” is not a good word choice. Malicious traffic must be detected because it requires investigation and discovery. Vendor remote access is granted by the entity and the entity provides the method by which remote access is performed. The method enabling remote access must have the ability to enumerate remote access sessions. Suggestion: The method enabling vendor-initiated remote access must have the ability to enumerate connected remote access sessions. **CIP-005, R3.2** An “established vendor” is a vendor that has been in business or a long time. How long does a session have to be active before it is widely considered to be established? The intent is to terminate a “connected” session. Suggestion: Have one or more method(s) to terminate connected vendor-initiated remote access sessions.

Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT modified the use of the word "detecting". The SDT has considered concerns about the use of “vendor-initiated” and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT appreciates that Platte River Power Authority has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
It isn’t as clear as it could be. Diagrams of the different scenarios would certainly help to clarify. Additionally, suggest replacing the word “Detect” as this implies the vendor is trying to make a remote connection without any permission from the Responsible Entity. Suggested wording for R3, Part 3.1: Have one or more methods for “establishing and monitoring” vendor-initiated remote access sessions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the requirement to remove the use of the 'detecting'. The SDT will also consider diagrams of different scenarios as improvements to the IG and TR to bring further clarity.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term "remote access" is not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GSOC and GTC recommends that the SDT either: (1) collaborate with the appropriate, assigned SDT to modify the definition of "Interactive Remote Access" as necessary to ensure that it incorporates the necessary language or (2) create newly defined terms for "vendor-initiated remote access" and "vendor-initiated system-to-system access." GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The word 'remote' is embedded within certain enforceable Glossary of Terms definitions, and it is outside the scope of the 2019-03 SAR to define terms that would have a broader reaching impact outside the scope of the supply chain risk management standards. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	

MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited.	

Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees that having EACMS access does not mean the EACMS has been exploited. The intent is to mitigate the risk that vendor remote access to an EACMS poses to the associated BES Cyber Systems. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Question 1 for Independent Electricity System Operator	

Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not mean the device has been exploited. Moreover, the term "remote" in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments, which were identical to those submitted by the EEI comments. Please see the SDT's response to EEI's comments.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
See response to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Refer to the SDT's response to Question 1 for Ameren - Ameren Services	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. It is not the intention of the SDT to expand the context of remote sessions. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity. The SDT appreciates that Lower Colorado River Authority proposed suggestions to help bring clarity. The SDT considered these suggestions when preparing the 3rd draft. The 2016-02 SDT is in the process of proposing revisions to the term Interactive Remote Access (IRA) in order to address NERC V5-TAG issues, and virtualization which proposes to replace existing ESP/EEP concepts with 'logical isolation' to enable the use of emerging technologies while maintaining backwards compatibility. For these reasons, the 2019-03 SDT has chosen not to create a variant to a currently defined term that is undergoing modification and is also perceived by many as ambiguous today in favor of clarifying language within the Applicable Systems and requirement language.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The proposed revisions do not clearly define the types of remote sessions that are covered by the standards and have the potential to be construed as broadening the potential interpretation of the types of vendor-initiated remote access sessions to which the requirements would apply. More specifically, the term "remote access" is not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks your for your comments, please see response to EEI Comments.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

The term "detecting" in part 3.1 - whereas an entity is required to "Have one or more methods for **detecting** vendor-initiated remote access sessions" implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must "detect" when they access the BCS. What is the security value in detecting a vendor who is already authorized to access the BCS?

A person accessing a system, vendor, or other should be addressed in CIP-004. The identification of a vendor system should occur in CIP-002. This also maps to ISO and NIST cyber security frameworks.

Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations a need may arise for vendors to initiate and establish remote access to an entities BCS, however a voice call to authenticate may be a better control.

Secondly, the words "established sessions" are an improvement from the language in the first draft; however, while this solved the problem posed by "disabling active sessions" where an idle session could remain enabled, it created another gap through the introduction of the word "initiated". The qualifier "initiated" may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" and "capability to use" the established session that is the risk regardless of which end initiated it.

Recommend alternative language that focuses on the risk itself or consider: Requirement R3 Part 3.1. "Have one or more methods for detecting established vendor remote access sessions." Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". In this case "terminating established vendor remote access sessions" is one way "how" an

entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket. Consider language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Modifications to CIP-002 and CIP-004 are out of the scope of the 2019-03 SAR. The SDT considered the comment on use of the word 'detecting' and has modified the standard to remove "detecting” The SDT also made additional changes to CIP-005 R3 to address the questions around "established sessions". Finally, the SDT considered the change of adding "vendor initiated" and understands that risk may be different when remote access is started from vendor equipment vs. entity equipment.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports EEI comments.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what “vendor-initiated” actually is. It would be beneficial to leverage language of Interactive Remote Access such as “Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)”.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. James Baldwin submitted identical comments. Please see the SDT's response to Lower Colorado Authority's comments submitted by James Baldwin.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST does not agree that the desired clarity has been achieved. N&ST recommends that the SDT consider a more detailed breakdown of R3 requirement applicability to help Responsible Entities distinguish between types of "vendor remote access" that DO require Intermediate Systems and types of "vendor remote access that do NOT, as CIP-005 is currently written, require Intermediate Systems: Intermediate System required: Vendor remote access that meets the current NERC definition of "Interactive Remote Access" and is therefore subject to CIP-005 R2. Intermediate System not required: Vendor remote access that does not meet the current NERC definition of "Interactive Remote Access." This includes system-to-system remote access and all types of vendor-initiated remote access to EACMS and PACS devices for which CIP-005 R2 is not applicable. One way to address this might be to break R3 part 3.1 into two sub-parts: Part 3.1.1 would be applicable to High Impact BES Cyber Systems and their associated PCA as well as Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA (Note the applicability is IDENTICAL to CIP-005 R2). Part 3.1.2 would be applicable to EACMS and PACS associated with High Impact BES Cyber Systems and with Medium Impact BES Cyber Systems with External Routable Connectivity that are not subject to CIP-005 R2.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. N&ST's comments for Question 2 were identical to the comments submitted for Question 1. Please refer to the SDT's response to N&ST's comment for Question 1.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
As written, see comments to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Eversource Energy	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	

Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
As written, see comments to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Hydro-Qubec Production.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

The proposed revisions do not clearly define the types of remote sessions that are covered by the standards. CIP standards need to use consistent language, define unclear terms and not leave so much to interpretation if requiring specific actions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Refer to responses to Question 1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Refer to the SDT's response to Question 1 for Cogentrix Energy Power Management, LLC	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree that the changes clearly define the types of remote sessions. There is still some ambiguity on what would be considered remote if the entity is to disable remote access to the very things that are used to define what remote access actually is. Would a remote user who attempts to get to an asset but is not authenticated and authorized, but made it to the asset that denies access, is that still considered access? The security which denies the access, such as a firewall, simply does not allow the access. However, there would be a log that is collected of the attempted access as well as any access that is authenticated and authorized.	
Likes 0	
Dislikes 0	
Response	
CIP-005-7 R2 Part 2.1 is bound by its applicability to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber System with External Routable Connectivity and their associated PCAs. The inclusion of EACMS and PACS in the Applicable Systems of CIP-005-7 R3 does not supersede nor modify the scope of the Applicable Systems CIP-005-7 R2 Part 2.1, and the use of an Intermediate System for EACMS and PACS is not required. EACMS by definition are a 'system', or collection of Cyber Assets that perform the EACMS functions. A user request to access part of an EACMS to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS. A packet at the NIC of an EACMS intended to establish a session that is later denied by the EACMS does not constitute 'access' into nor through the EACMS.	

The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Tacoma Power's comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The proposed changes do not provide clarity. Although the addition of "initiated" is appreciated, the removal of the IRA and system-to-system qualifiers introduces ambiguity. It is unclear whether "all" remote access sessions must be included or if the Entity has the authority to define "vendor-initiated remote access sessions," potentially reducing the scope of requirement. The removal of IRA and system-to-system is also inconsistent with the language changes to CIP-013-2, R1.2.6.	

Additionally, the "Measures" were not updated to reflect the proposed changes. Specifically, the "Measures" still include the language from the original CIP-005-2 R2.4 and R2.5 requirements "active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access." ISO-NE recommends keeping the "initiated" qualifier, adding terms or information to clarify the specific in-scope remote access sessions, and ensuring consistency with CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
LaTroy Brumfield - American Transmission Company, LLC - 1	

Answer	No
Document Name	
Comment	

ATC agrees the words "established sessions" are an improvement from the language in the first draft; however, while this solved the problem posed by "disabling active sessions" where an idle session could remain enabled, it created another gap through the introduction of the word "initiated". The qualifier "initiated" may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" and "capability to use" the established session that is the risk regardless of which end initiated it. ATC requests consideration of alternative language that focuses on the risk itself. Another potential solution to consider could be the following: Requirement R3 Part 3.1. "Have one or more methods for detecting established vendor remote access sessions." Requirement R3 Part 3.2. "Have one or more method(s) to revoke the ability for a vendor to establish and use remote access". If this were the language, then "terminating established vendor remote access sessions" is one way "how" an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language.

Additionally, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of read-only "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). Consequently, established non-persistent read only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the "vendor remote access" bucket. ATC requests consideration of qualifying language to exclude non-persistent read only information sharing sessions (i.e. WebEx) from being considered "access" to prevent CIP-011 from creeping into CIP-005.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT appreciates that it has proposed some potential language to address this concern and considered those suggestions when preparing the 3rd draft. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD agrees with Tacoma Power, please refer to their comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to Tacoma Power's comments.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	

Oncor supports the comments submitted by EEI. In addition, there is a conflict between the language in CIP-005-7, R3 and CIP-013-2 inasmuch CIP-013, R1.2.6 takes out "Interactive", and "with a vendor" in terms of remote or system to system access, but then the changes to CIP-005-7 do not match the changes in CIP-013-2, R1.2.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to EEI's comments.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 1 for Con Ed - Consolidated Edison Co. of New York.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	

The changes to the newly formed R3 appear to have had the opposite effect of clearly defining the types of remote sessions. With these changes, there is no clarity about what a vendor-initiated remote access session is. Does “access” refer to read-only access? Or does “access” only refer to control? What is the meaning of “remote” in this situation? “Remote” to an applicable system? How is that clarified? Tacoma Power does not support these changes to CIP-005 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of “vendor-initiated” and recognizes the risks may be different based on the use of vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to ‘a lower trust level system external to the Applicable Systems it is connecting into or through’, and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

While the SDT is coming at this from the supply chain aspect, the technical application of the mechanisms to detect, terminate and disable remote access sessions requires the ability to do it for any remote access session; therefore the specific language "active vendor remote access" and "includes vendor-initiated sessions" is of no practical value. If the entity has the ability to detect, terminate, and disable remote access sessions, they have the ability do this for vendors or for insiders. In BPA's opinion, there is no point in making the requirement strictly about vendors. It could as easily be applied to partners, customers, remote employees, etc., and to the same benefit in reduced risk to the reliability and secure operation of the grid.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT appreciates the security focus that remote access should be treated similarly, however, this is a critical distinction that is necessary, especially in the context of union agreements where an entity could be faced with an impossibility of compliance if required to monitor activity and detection of established of union personnel. Additionally, it stands to reason that vendor remote access, as a function of its risk, be treated differently and more rigorously than remote access by the entity. For these reasons, the SDT was mindful to separate out vendor remote access to assure the activity monitoring and session detection components of vendor access are not extended to an entity's employee base.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
No, Santee Cooper does not believe that the changes in CIP-005-7 R3 clarify remote session conditions. If this is the SDT's intent, then they should define vendor-initiated remote access. In CIP-013-2 two different remote access conditions are mentioned vendor-initiated remote access and system to system remote access. Whereas in CIP-005-7 only vendor-initiated remote access is mentioned.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 and has worked to align that language.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The current language in CIP-005-7, Requirement R3 does not sufficiently describe what constitutes, or clarifies the meaning of, a remote session within the context of an EACMS. Specifically, having access to an EACMS does not equate to the device being exploited. Moreover, the term “remote” in the context of an EACMS, such as an Intermediate System, is unclear given Intermediate Systems, by definition, must be remote from an Electronic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, which were identical to those submitted by the EEI comments. Please see the SDT's response to EEI's comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments	

The term “detecting” in part 3.1 - whereas an entity is required to “Have one or more methods for **detecting** vendor-initiated remote access sessions” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” when they access the BCS. What is the security value in detecting an entity which is assumed to already be authorized to access the BCS? Recommend considering preventive controls to authenticate vendor sessions. This could be administrative processes such as sharing a code word, verifying vendor change ticket numbers, pre-confirmed call-out lists, confirming an authentication code (such as RSA token), or technical controls such as Identity and Access Management controls. In some emergency situations, a need may arise for vendors to initiate and establish remote access to an entity's BCS, however, a voice call to authenticate may be a better control. Secondly, the words “established sessions” are an improvement from the language in the first draft; however, while this solved the problem posed by “disabling active sessions” where an idle session could remain enabled, it created another gap through the introduction of the word “initiated”. The qualifier “initiated” may have unintended consequences that defy the security objectives. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access, retention of established sessions, and the ability to re-establish sessions (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” and “capability to use” the established session that is the risk regardless of which end initiated it. Recommend alternative language that focuses on the risk itself or consider: Requirement R3 Part 3.1. “Have one or more methods for detecting established vendor remote access sessions.” Requirement R3 Part 3.2. “Have one or more method(s) to revoke the ability for a vendor to establish and use remote access”. In this case “terminating established vendor remote access sessions” is one way “how” an entity could meet this objective (although it highlights the gap in the existing draft that terminating an established session alone may not preclude the re-establishment of another session), hence the need to adjust this language. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of read-only “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established non-persistent read-only sessions (i.e. WebEx) between a Registered Entity and a vendor are being lumped into the “vendor remote access” bucket. Consider language to exclude non-persistent read-only information sharing sessions (i.e. WebEx) from being considered “access” to prevent CIP-011 from creeping into CIP-005.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. Modifications to CIP-002 and CIP-004 are out of the scope of the 2019-03 SAR. The SDT modified the used of the word 'detecting' in CIP-005 R3. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different with the use of vendor equipment vs entity equipment. The SDT appreciates that MRO NSRF has proposed some potential language to help clarify where CIP-005-7 R2 is applicable and will consider the suggestions made when preparing the next proposed draft. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	

Comment
No, the changes made it worse by including the definition of a session in the measure and not in the requirement itself. As written in part 3.1 entities have to detect "vendor-initiated remote access sessions" without indication on what this includes. It is vague language. In the measure a definition is given for an active vendor remote access session as "including system-to-system, as well as interactive remote access, which includes vendor-initiated sessions". Requirements cannot be buried in glossary definitions or measures as it implies a rule without be an explicit rule. The definition needs to be placed back into the requirement itself.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT moved the IRA and system to system access qualifiers out of the requirement language and into the measures in CIP-005-7 Requirement R3 to address a perceived concern of a 'hall of mirrors'.

The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The Measures detailed in the Requirement Parts do clearly define the types of remote sessions that are covered by the standards. However, the Measures language does not use the same terminology ("vendor-initiated" connections) that is used in the Requirements language, which may lead to confusion. WECC recommends removing the term "vendor-initiated" as discussed in the previous comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT has considered concerns about inconsistencies between the language in CIP-013-2 and CIP-005-7 as well as the Measures and has worked to align that language.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State does find the addition of the phrase "vendor-initiated" helpful, however we think it still leaves too much room for interpretation. To further clarify, we recommend a few additional edits: 1) In the measure for part 3.1, recommend changing the language "(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)" with "(either via system-to-system remote access or Interactive Remote	

Access, and which is initiated from a vendor's asset or system)", and 2) In the requirement itself, we recommend adding something like the following to end of the drafted requirement language ", whether via system-to-system remote access or Interactive Remote Access." Similar edits should be made to part 3.2. Finally, we ask that the drafting team consider adding a statement to help clarify and address the various emerging regional interpretations regarding web conferences, either in the core requirement R3, or under both parts 3.1 and 3.2. To that end, we recommend adding a statement to this effect "Remote sessions initiated by the responsible entity's personnel, where the vendor has no control, is not in scope".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks may be different when using vendor equipment vs entity equipment. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT has not defined remote because it carries context in its usage and relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The words "vendor-initiated remote access sessions" are not properly defined and are ambiguous. "Sessions" could be taken as exclusive to TCP Only connections or could mean any connection such as a serial HyperTerminal session … etc.

R2 strictly discusses vendor-initiated remote access. If an entity initiates the remote access via a WebEx and gives control to a vendor the access should then be considered vendor initiated and follow R3 requirements.

Does the vendor-initiated remote access include non-routable vendor-initiated communications Consider including communications such as dial-up, serial, corporate TTY terminal servers to EACMS and PACS, etc. Perhaps modify requirements to state P3.1 – " Have one or more methods for detecting all vendor sessions, regardless of protocol, type of connection, or initiation" and P3.2 - "Have one or more methods to terminate all vendor sessions regardless of protocol, type of connection, or initiation"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has considered concerns about the use of "vendor-initiated" and recognizes the risks could be higher from vendor equipment vs entity equipment. The word 'remote' refers to 'a lower trust level system external to the Applicable Systems it is connecting into or through', and when used in the phrase vendor remote access it refers to those systems or personnel from a vendor. The SDT relies on the scoping identified in the Applicable Systems for each Requirement Part. The SDT agrees read only WebEx sessions are lower risk than command and control and considered comments to add clarifying language or qualifiers to the phrase vendor remote access to help bring the needed context into the requirements, and to clarify the variance in risk associated with a read-only session vs giving a vendor control. The SDT will also consider improvements to the IG and TR to bring further clarity.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
As written, see comments to question 1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Refer to the SDT's response to Question 1 for New York Power Authority.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree that the proposed language clarifies remote session conditions. Duke Energy, is concerned about the new wording for R3.1, specifically the change of “determined” to “detecting”. This leaves open a question if the intent is continuous monitoring for or detection of sessions, on-demand or periodic detection, or just detection upon initiation.	
Likes 0	
Dislikes 0	
Response	
The SDT modified the use of the word ‘detecting'.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding "vendor-initiated…".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Though CAISO supported the addition of 'vendor-initiated', the SDT received several industry comments with concerns regarding the addition of 'initiated' and the SDT considered those comments.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	Yes
Document Name	

Comment	
The IRC SRC believes that the proposed language under R3 more clearly defines the type of remote sessions that are covered by adding "vendor-initiated…"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Though MISO supported the addition of 'vendor-initiated', the SDT received several industry comments with concerns regarding the addition of 'initiated' and the SDT considered those comments.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Snohomish County PUD No. 1 did not provide comments for Question 2.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to the proposing language in Part 3.2, but disagree the term “detecting” in Part 3.1 since “detecting” implies an entity is not aware of the instances of when a vendor is remotely accessing their BCS and must “detect” them. We suggest changing from “detecting” to “verifying”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has modified the requirements to remove the 'detecting'. This aligns with the FERC Order to extend protections to EACMS and PACS without modifying the original intent of the Requirement.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments to #1.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	

Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 7 for Northern California Power Agency.	

3. The SDT is proposing removing the exception language in CIP-010-4 "Applicable Systems" for PACS which stated "except as provided in Requirement R1, Part 1.6." This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented

on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.	
Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Question does not address the proposed addition of EACMS and PACS to the CIP-10-3 R1.6 requirement. ISO-NE does not agree with adding EACMS and PACS to the "Applicable Systems." The additions potentially exceed the FERC order, which can be interpreted to only extend the supply chain requirements to the CIP-013-1 Standard. Given the CIP-010-3 R1.6 requirement is not even effective yet, there is insufficient evidence to support further expansion into a CIP environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards..." Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security –	

Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-005-7 and CIP-010-4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC/GSOC do not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GTC/GSOC assert that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GTC/GSOC oppose the inclusion/addition of PACS to the supply chain reliability standards. While GTC/GSOC understand the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, they believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to GSOC's comments.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	

Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC and GTC does not support any revisions that have the result of including PACS in the requirements of interest in this project. Various reliability standards already mitigate security risks relating to PACS, e.g., CIP-004-6; CIP-006-6; CIP-007-6; CIP-009-6; CIP-010-2; and CIP-011-2. GSOC and GTC asserts that these protections are sufficient given the attenuated relationship that a PACS compromise has to BES reliability impacts. For these reasons, GSOC and GTC remains opposed to the inclusion/addition of PACS to the applicable supply chain reliability standards. While GSOC and GTC understands the potential risks identified by NERC in Chapter 3 of its Supply Chain Risks report, we believe that these risks are already appropriately mitigated through the protections that are mandated for PACS within the existing set of CIP reliability standards.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and	

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through

a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose. Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013. Also, too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven. The IRC SRC believes that requirement R1.6 should be applied to other Cyber Assets. Making a regulatory compliance requirement for a subset of assets in the enterprise increases the cost of implementation and maintenance dramatically to a point that it may be detrimental to the overall company security posture, ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS and PACS to the R1.6 requirement as this requirement has not yet proven to be effective as it stands.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with	

medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-010-4 and CIP-005-7.

The SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".
In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.
The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.
Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect. Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC believes the question should solicit comment as to the proposed addition of EACMS and PACS of draft 1 which we oppose.

Second, the IRC SRC believes the addition of EACMS and PACS to the scope of CIP-005 is more than what was directed in the FERC order. The FERC order was limited to the extension of supply chain requirements under CIP-013.

Also, it is too early to add more requirements when a standard has not been put into place yet, the cost to the industry is unknown and its effectiveness is unproven.

it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Per FERC Order No. 850 paragraph 5, the 2019-03 SDT has mandatory directives to address this gap, "...pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…" Where paragraph 1 of the same FERC order defines the supply chain risk management Reliability Standards to include CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)." For these reasons, the inclusion of EACMS and PACS are within the scope of the FERC order and the SDT must address vendor remote access into EACMS and PACS within both CIP-010-4 and CIP-005-7.

The SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".
In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk. Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect. Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves. The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with reverting the language in this section back to what is in CIP-010-3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree to remove the specific language in the Background section to clarify the applicable PACS.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments.	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Snohomish County PUD No. 1 did not provide comments for Question 3.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA agrees that this reads better with the language removed. However, if we are looking at this from a Supply Chain perspective perhaps we should consider removing with "External Routable Connectivity" and evaluate all PACS as they are being procured.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PACS are not currently required for medium impact BES Cyber Systems without External Routable Connectivity, and the removal of ERC would have broad ranging impacts to the suite of CIP Cyber Security Standards and is not in scope for the 2019-03 SAR.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	

The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
No additional comments on this question.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern does not have any issues with the removal of the exception language in the Applicable Systems for PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Answer should have been "No". We do not su[pport adding PACS.	
Likes 0	
Dislikes 0	
Response	
he SDT appreciates the comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and	

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6 We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

The redline-to-last-posted does not show any changed to Part 1.6 We agree that the SDT followed the Directive's instructions	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to MRO NSRF's comments.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes

Document Name	
Comment	
Removing this specific language helps entities to clarify the requirements pertaining to each applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
The redline-to-last-posted does not show any changed to Part 1.6. We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. That is correct. The SDT did not make any further modifications to the 2nd draft of CIP-010-4 Requirement R1 Part 1.6 in response to the initial ballot, and the proposed changes remain the same to add EACMS and PACS to the Applicable Systems without modification of the language itself in CIP-010-4 Requirement R1 Part 1.6. The modifications for the second ballot were limited to the removal of the exception language from PACS in Background (Section 6) of the Standard to address industry comments related to the confusion this caused.	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	Yes
Document Name	
Comment	
We agree that the SDT followed the Directive's instructions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see respond to question 7.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	

Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks your for your comments, please see response to EEI Comments.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

Cyber Security Supply Chain Risk Standard Drafting Team Summary Response:

CIP-013-2 is a risk-based standard that requires an Entity to develop and implement a supply chain cyber security risk management plan. The Entity's plan should include process(s) for procurement that address minimum requirements listed in R1.2.1-R1.2.6. This requirement is about a plan and ensuring the controls are coordinated between the Entity and the Vendor, and is intentionally not prescriptive in order to allow the Entity enough flexibility in developing their specific plan(s) and process(es).

CIP-005-7 3.1 and 3.2 language has been updated. CIP-13-2 R2.1.6 also has been updated to clarify vendor-initiated remote access, and more closely align with the new proposed revisions to CIP-005-7.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to NPCC RSCC.	

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is no clear definition of what is a vendor-initiated, remote access and system-to-system remote access. SRP would like to see the definitions clearly defined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is supporting the IRC SRC Comments as follows: The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
The IRC SRC believes that the reconstructed wording of requirement R1, Part 1.2.6 is Inconsistent with the proposed changes to CIP-005. It is not clear of what types of remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
Removing "Interactive" creates ambiguity and negates the need for having a (i) and (ii). The result is (i) remote access, and (ii) system-to-system remote access (which is a subset and included within (i) remote access). Without "Interactive" (ii) is redundant. The resulting requirement then would be, "Coordination of controls for vendor-initiated remote access". The term "remote access" is unclear and must be further defined. That is why the original language clarified "remote access" using "Interactive Remote Access" (a defined term) and "system-to-system remote access" (commonly understood). Suggestion: define the term "remote access" or put "Interactive Remote Access" and "system-to-system remote access" back into the requirement.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
This creates more confusion as CIP-005-7 refers to IRA and vendor remote access. Need to correlate that if the vendor uses IRA, requirements in R2 apply. Correct? Otherwise vendor remote access (system to system) must be through an EAP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
For the reasons indicated above, GSOC and GTC respectfully reiterates that revisions to strip the requirements down to generic terms like "remote access" and "system to system access" have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms "remote access" and "system to system access" are not defined and, even as modified by the term "vendor-initiated," could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate	

system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GSOC and GTC does not agree that the proposed revisions make clearer the types of remote sessions that are covered by the standards. GSOC and GTC further reiterates its previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access. Examples: • If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. • If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican Energy Company agrees with considering vendor-initiated remote access. However, the standard language should address the intent versus the capability. Further, we recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the version proposed. Even if the vendor could potentially gain access, such as by requesting control during a WebEx meeting, that is not vendor-initiated remote access. Examples: · If the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. · If the intent is to show a user's computer for trouble-shooting or other reasons, then this is read-only access managed by the Entity and not subject to the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We believe that the proposed wording changes for R1.2.6 unnecessarily broaden the scope of this requirement. The term "interactive" is key to the wording of this requirement and consistent with the usage of IRA elsewhere in the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	

The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what "vendor-initiated" actually is. It would be beneficial to leverage language of Interactive Remote Access such as "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
For the reasons indicated above, GTC/GSOC respectfully reiterate that revisions to strip the requirements down to generic terms like "remote access" and "system to system access" have the potential to be construed as broadening the potential interpretation of the types of remote access sessions to which the requirements would apply. More specifically, the terms "remote access" and "system to system access" are not defined and could be construed as access from outside an entity's network, access from outside of the Electronic Security Perimeter within which the assets resides, access through an intermediate system, or any other access that is initiated by a vendor and that does not directly access the applicable asset. This potential for ambiguity and confusion could lead to significantly different implementations and interpretations by both registered and regional entities (as applicable). For this reason, GTC/GSOC do not agree that the proposed revisions makes clearer the types of remote sessions that are covered by the standards. GTC/GSOC further reiterate our previous comments regarding the unsupported addition of PACS to this requirement.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT's summary response under question 4.	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: "Coordination of controls for all vendor-initiated remote access." We believe that specifying and breaking down remote access types (e.g. "system to system") adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Without a definition of what System to System remote access is, the changes requested do nothing to clarify anything different that was written in version 2. A definition for system to system remote access needs to be created and added to the Glossary of terms. While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word "initiated" may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that	

established session is moot. It is the "presence of" the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). This is evident where established read only sessions between a Registered Entity and the vendor are included as "vendor remote access." Recommend language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered "access" to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the notion that vendor-initiated remote access should be considered. We feel that the standard language needs to address capability versus intent of the remote access. Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions. If a vendor has the capability of implementing changes on a BCS shifts because the vendor is participating in an activity where control of the user's computer could be granted to the vendor (WebEx for example), then this isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The changes to the SCRM Standards expanded remote sessions. In the proposed version, "vendor-initiated remote access sessions" has been added. This creates some confusion on what "vendor-initiated" actually is. It would be beneficial to leverage language of Interactive Remote Access such as "Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP)".	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST does not agree that the desired clarity has been achieved. N&ST recommends simplifying Part 1.2.6 to read: "Coordination of controls for vendor-initiated remote access to applicable systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT's summary response under question 4.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. . We recommend consistency between these Standards and defining terms such as "interactive remote access" and "remote access".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We do not agree that the proposed language clearly defines the intended types of vendor remote access. First, we do not agree that Interactive Remote Access vendor sessions should be treated differently than internal sessions. Second, Part 1.2.6 (ii) specifies system-to-system remote access but the language is not bound to vendors. The requirement could be interpreted to include all system-system remote access, vendor or internal.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree with the reconstructed wording. The updated text causes further confusion from the original. During the WebEx it was discussed that IRA and system-to-system are sub-sets of vendor remote access. To ensure clarity, Southern would like the SDT to consider the following possible rewording: "Coordination of controls for vendor-initiated (i) Interactive Remote Access, and (ii) system-to-system remote access to BES Cyber Systems. Another requirement for consideration would be to add the following, "1.2.7 Coordination of controls for vendor-initiated remote access (interactive user access and system-to-system access) to applicable EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE recommends review of the proposed CIP-005-3 changes to ensure consistency.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy supports the notion that vendor-initiated remote access should be considered in CIP-013-2 R1, P1.2.6; however, we feel that the standard language needs to address the capability of the vendor while having access versus the intent of the vendor's remote access. Meaning, if the intent of the remote access is to perform operational activities on a BES Cyber System, then that vendor initiated remote access is in-scope for this requirement. This kind of remote access can be contemplated during contract scoping discussions. However, there is an ambiguity when it comes to the remote sharing applications between Entity and Vendor (i.e. webEX, Skype, Zoom, etc.), in that during these remote sharing events, a user's (Entity) computer can grant to the vendor control of their screen. NV Energy believes that this event isn't classified as vendor-initiated remote access with regards to the objective of the standard. We recommend continuing to use the term Interactive Remote Access to address the remote access scoping issues related to the current version proposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment	
The use of the word “initiated” may have unintended consequences that defy the security intent. If the goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the “presence of” the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. ATC requests consideration of alternative language that focuses on the risk itself. Additionally, the phrase “vendor remote access” is ambiguous because it is undefined and the word “access” is broad. As a result, emerging interpretations are blending the concepts of “information sharing” sessions (CIP-011) with the concepts of BCS “access” sessions (CIP-005 & CIP-007). Consequently, established read only sessions between a Registered Entity and the vendor are being lumped into the “vendor remote access” bucket. ATC requests consideration of qualifying language to exclude established non-persistent read only sessions (i.e. WebEx) from being considered “access” to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT’s summary response under question 4.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
While the SDT does a good job in reconstructing the wording, it only addresses “’vendor” and “system-to-system” access. Remote access to BES Cyber Assets and Systems can be granted by the entity to not only its employees, but to its vendors and contractors, separate and outside from access granted to other vendors or systems.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
It is better to use the defined terms that are used throughout the standards. Using "remote access" instead of "Interactive Remote Access" implies what is being addressed in this requirement different than Interactive Remote Access in ways other than being vendor-initiated. Also, the source of initiation is not clear with system-system remote access, but if a vendor is compromised, any system-to-system remote access with that vendor should be terminated without regard to who initiated it. The original language is better.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
To enhance general applicability to all vendor-initiated remote access, suggest: "Coordination of controls for all vendor-initiated remote access." We believe that specifying and breaking down remote access types (e.g. "system to system") adds confusion and decreases clarity with respect to securing all manners of vendor-initiated remote access.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
The changes to CIP-013-2 Part 1.2.6 appear to have had the opposite effect. Now there is no clarity about what a vendor-initiated remote access session is. Does "access" refer to read-only access? Or does "access" only refer to control? What is the meaning of "remote" in this situation? "Remote" to an applicable system? How is that clarified?	

Additionally, it appears that (ii) system-to-system remote access, is now just a subset of (i) remote access. Tacoma Power does not support these changes to CIP-013 and recommends creating one or more defined terms to help provide clarity in this situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes "Coordination of controls" remains somewhat ambiguous. Inclusion of "vendor-initiated" for both remote access and system-to-system remote access is somewhat redundant and confusing. BPA proposes the following: *1.2.6. Coordination of remote access controls for vendor personnel or systems accessing BES Cyber Systems ESP/ESZ to include; reasons and requirements for remote access, periodicity of access (temporary or permanent), methods of authentication, and revocation processes for personnel.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No

Document Name	
Comment	
The SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 that all types of vendor-initiated remote access need to be considered then the wording used in CIP-005-7 should be consistent with the wording used in CIP-013 R1, Part 1.2.6. In CIP-005 "vendor initiated remote access" is used while both "vendor initiated remote access" and system to system remote access is used in CIP-013 R1, Part 1.2.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	

Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments While this revision clarifies the considerations for remote access controls in supply chain risk management plans and processes, the use of the word "initiated" may have unintended consequences that defy the security intent. The goal is to implement controls that prevent or mitigate the risk of unauthorized access (whether interactive or system-to-system) by a remote vendor then the initiator of that established session is moot. It is the "presence of" the established session that is the risk regardless of which end initiated it once the Registered Entity determines that vendor should no longer have that access. Recommend language that focuses on the risk itself. Similar, the phrase "vendor remote access" is ambiguous because it is undefined and the word "access" is broad. As a result, emerging interpretations are blending the concepts of "information sharing" sessions (CIP-011) with the concepts of BCS "access" sessions (CIP-005 & CIP-007). This is evident where established read-only sessions between a Registered Entity and the vendor are included as "vendor remote access." Recommend language to exclude established non-persistent read-only sessions (i.e. WebEx) from being considered "access" to applicable systems to prevent CIP-011 from creeping into CIP-013 where the scope is supposed to be limited to high and medium impact BES Cyber Systems and their associated EACMS and PACS.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
CIP-013-2 R1, Part 1.2.6 requires one or more processes used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access. This language provides the two basic types of vendor remote access; however, it lacks the detail provided in CIP-005-7 R3, Parts 3.1 and 3.2, which may be required to effectively assess risk. Further, as discussed in the previous comments, the use of the term "vendor-initiated" is troubling because it should not matter whether the vendor or the entity initiates the connection. By considering only vendor-initiated connections, the language omits some vendor remote access connections, and therefore does not meet the security objective of the Requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State does not agree with the changes; we believe the CIP-013-1 language is more clear and comprehensive.

The previous CIP-013-1 wording

• “Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)”

is more clear and more comprehensive than the proposed CIP-013-2 wording

• “Coordination of controls for vendor-initiated (i) remote access, and (ii) system-to-system remote access.”

CIP-013-2’s “Coordination of controls for vendor-initiated … system-to-system remote access” seems to exclude system-to-system remote access that’s internally-initiated, where a system inside the ESP automatically creates a remote access session with a vendor’s system in the vendor’s network.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the SDT’s summary response under question 4.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders’ time on this

endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with

trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods. 2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions. 3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard. 4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.	
Erick Barrios - New York Power Authority - 6	
Answer	No
Document Name	
Comment	
We recommend that any changes to CIP-005 need to be consistent with changes here. CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	

Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees with clarifying that all types of vendor-initiated remote access needs to be considered. Texas RE recommends that the term "vendor" be defined in the NERC Glossary. Although it is defined in the Supplemental Material, that material is not part of the standard and is not enforceable. There is still confusion on who and what is a vendor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
EEI supports the notion that all vendor-initiated remote access should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	

Evergy (Westar Energy and Kanas City Power & Light Co.) supports the position that all vendor-initiated remote access needs to be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
We agree with this revision that clarifies vendor-initiated remote access controls in supply chain risk management plans and processes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the reconstructed the wording clarifies that all types of vendor-initiated remote access needs to be considered.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	

ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	

Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's summary response under question 4.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

Thank you for your comment. Based on the items listed below. The SDT determined that 18 months is sufficient. The SDT expanded the implementation time to 18 months based on the following criteria:

- EACMS and PACS represents a significant expansion in scope for both hardware and software that may undergo planned procurement.
- While CIP-013-2 does not require the Responsible Entity to renegotiate or abrogate existing contracts there is a recognition that (the large number of vendors and their contracts that are currently in place may need to be modified and renegotiated to cover any new existing equipment and systems that would need to be put in place.
- Vendors are possibly placed in several regions and jurisdictions and would take more time to consolidate the same policies and procedures across the entity.

In addition to the above, some entities expressed the consideration of budget cycles due to technological upgrades needed for the implementation along with the budgeting and planning efforts within most entities occur annually with the planning and finalization occurring a year in advance. Those technology upgrades may include but not be limited to:

- Implementing a Governance, Risk, and Compliance (GRC) solution if not already deployed within their organization.
- A Third Part Risk Management (TPRM) solution in concert with the entities' Supply Chain Management.

An 18-month implementation plan would allow organizations to address any change management, possible contract revisions, vendor additions, budget cycles, and policy modifications to be put in place in a timely manner.

Regarding the comments around COVID-19, the SDT believes that 18 months provides adequate time to implement the revisions as well as accommodate issues resulting from the pandemic response in accordance with the NERC-issued guidelines that entities may leverage if COVID-19 materially impacts any ability to comply with periodic requirements or future enforceable standards.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	
Comment	
We think 24 months better supports the process we have at a small utility with minimal IT resources.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Due to the Covid-19 impacts to industry, we suggest considering a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response:

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments

Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24-month implementation plan.

Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
It appears that the basis for the originally proposed 12-month implementation centers on an assumption that EACMS and PACS vendors are the same for high impact and medium impact BES Cyber Systems. This supposition would make it appear that it is a straightforward expansion of existing Supply Chain programs to EACMS and PACS. This is not true in all cases. Notably, the high impact (e.g. control center) and medium impact (e.g. substation) environments are very different. CEHE believes that such a difference justifies a longer implementation period. CEHE suggests that 18 months is not enough and proposes a 24-month implementation plan instead.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
These changes are adjustments to existing standards, and 12 months is plenty of time to implement the changes.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Due to the on-going Covid-19 impacts and delay of initial supply chain standards implementation, it is recommended to consider a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Wayne Guttormson - SaskPower - 1	

Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Due to the development of the virtualization standards, and supply chain standards implementation overall, we recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment	
Due to the Covid-19 impacts to industry, the virtualization standards under development, and supply chain standards implementation overall, it is recommended to consider a 24 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
MidAmerican appreciates the proposed increase to the implementation plan. However, we recommend consideration of a 24-month implementation plan in order to provide time for NERC to coordinate ongoing efforts of other SDTs that may also impact the supply chain standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	No
Document Name	
Comment	

In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with a longer implementation plan window.	
Likes 0	

Dislikes 0	
Response:	
Thank you for your support.	
Erick Barrios - New York Power Authority - 6	
Answer	Yes
Document Name	
Comment	
We agree with the SDT proposal	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response:	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports the 18 month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
NV Energy agrees that the the extension in implementation timeline is acceptable; however, with the expectation of revisions to the CIP Standards through Project 2016-02, and the concurrent work required to implement these future changes, NV Energy would request that NERC look to further extend this implementation timeline to ensure Entities have enough time to implement the concurrent revisions.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. The project 2016-02 is a separate project and will have a new implementation plan allowing entities to adjust accordingly once that project is completed. Please see the SDT response at the beginning of question 4 as to why 18 months is a sufficient timeframe for the Project 2019-03 Implementation plan.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes

Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) supports the 18-month implementation plan and the extended implementation period appropriate when considering the expanded applicability of the Standards.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Although 24 months would be more appropriate, GTC/GSOC appreciate the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO agrees with the increase of the implementation period from 12 moths to 18 months. IESO would prefer 24 months to take budget cycles into account. Although the we acknowledges that EACMS and/or PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and or PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
EEI supports the 18-month implementation plan.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your support.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Although 24 months would be more appropriate, GSOC and GTC appreciates the SDT's consideration of previous comments.	
Likes 0	
Dislikes 0	
Response.	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	Yes
Document Name	
Comment	

The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles.

Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.

Likes 0	
Dislikes 0	

Response:

Thank you for your comment. Please see the SDT response at the beginning of question 5.

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO is supporting the IRC SRC Comments as follows:

The IRC SRC supports the SDT changes to extend the implementation timeframe from 12 to 18 months. In addition, the IRC SRC requests the SDT consider an additional extension of the implementation timeframe to 24 months to accommodate budget cycles.

Although the IRC SRC acknowledges that EACMS and/or PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will

allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At this time, it is unknown whether the existing supply chain requirements will have a tangible improvement in supply chain security, so the IRC SRC recommends any expansion in the scope of requirements be deferred until more is known.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 5.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

SDT Response below:

Thank you for your comment. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP would first like to see the definitions that are outlined in CIP-005 and CIP-013 with more clarity and a better definition for each.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is supporting the IRC SRC Comments as follows:

Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.

Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3, Group Name NIPSCO	
Answer	No
Document Name	
Comment	

In order to properly evaluate and fund required changes a longer implementation period of 24 months is required. This is necessary to obtain possible funding and process changes that would be necessary.

Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks_June 2020	
Answer	No
Document Name	
Comment	
Although the IRC SRC acknowledges that EACMS and PACS are important to protect, we recommend NERC wait to extend the program to EACMS and/or PACS until after the CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the IRC SRC also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. While the IRC SRC believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory requirements should not be applied to additional Cyber Assets. When a regulatory compliance requirement is expanded to include additional assets in the enterprise, it increases the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. Therefore, the IRC SRC opposes adding EACMS or PACS to the supply chain requirement as this requirement has not yet proven to be effective as it stands.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
It's difficult to determine the cost since CIP-013 is not effective and no studies have been conducted to determine the cost to implement across the industry. Including PACS and EACMS adds another layer to consider once the BCS' Supply Chain Risk Management requirements are implemented. The scope continues to expand without consideration to the industry as a whole to first achieve the risk mitigations for the initial standards and without studies to determine the effectiveness of the Supply Chain Risk Management standards for BCS'. Unless small entities contract with 3rd parties for the vendor risk assessments required, what is their alternative since vendors usually do not respond to their cyber security questionnaires. Suggest determining the effectiveness of the first CIP-013 standards before adding more systems to the requirements and potentially adding additional costs.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While GSOC and GTC acknowledges the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The burden on the industry will increase with expanding the scope of these requirements to include EACMS and PACS. The cost of this burden cannot be credibly estimated at this time. Costs and benefits need to be considered for both the industry and vendors.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Support the comments of the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
While GTC/GSOC acknowledge the current flexibility in implementation that the CIP reliability standards provide, the inclusion of PACS in the CIP reliability standards would not be cost-effective as it will provide no direct benefits to the reliability of the BES. Further, as these systems are not included in the FERC directive, it is certainly not cost-effective to unnecessarily include them.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	
Comment	
The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No

Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
We do not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known..	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

The current language in the standard intentionally creates different expectations for vendor remote access versus internal staff remote access. As this subjects the entity to potentially multiple frameworks for the same activity, it inherently creates an inefficiency to the process that could be easily eliminated. Furthermore, the current measures in CIP-005 Part 3.1 introduce process activities that go beyond the stated requirements (i.e. monitoring remote access activity), potentially leading entities to implement more costly approaches to meet the standard requirements.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Although ISO-NE acknowledges that EACMS and PACS are as important to protect as the BCS in line with the FERC Order, we recommend to wait on extending the program to EACMS and PACS until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors to ensure they are implemented in the most cost-effective manner. At that time, the ISO-NE also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The larger inclusion of Cyber Assets (EACMS and PACS) increases the scope and burden on industry. The cost of CIP-013 compliance is currently unknown as this is a new standard. This potentially adds an additional set of Vendors/Supplier's that provide equipment, software, or service. Therefore, currently providing any credible cost or benefit information is premature. External increased costs imposed on industry by our vendors is also an unknown variance that cannot be predicted at this time	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
The ambiguity around what "access" is, what "remote" is, and what "vendor" is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18,	

2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, the CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Additional costs will be driven to add those new EACMS and PACS assets to supply chain overview.	
Likes 0	
Dislikes 0	
Response:	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Depending upon how an entity implements their initial Supply Chain Standards program, the proposed changes to CIP-005, CIP-010 and CIP-013 could result in significant impacts to an entity's program and may not be as simple as merely adding a few additional systems. For these entities, they may need to develop and implement a different process for EACMS and PACS systems.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
To minimize churn among standard versions, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-005-7, CIP-010-4, and CIP-013-2 with other existing drafting teams for related standards; specifically, Projects 2016-02, 2020-03, and 2020-04. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.	
Likes 0	

Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test, and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that	

reduces cost-effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result.

Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost-effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020, clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective-based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".

Likes 0	
Dislikes 0	

Response:

Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Inclusion of EACMS and PACS to CIP-005 R3 Part 3.1 will require significant investment to isolate these Boundary Assets to be able to monitor for and terminate vendor remote access sessions. This is a substantial change to definition of EACMS and PACS and likely will bring additional assets into scope by requiring entities to define the new boundaries and cyber security isolation methods that had previously not been required.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State recommends EACMS be separated into EACS and EAMS. Not separating the concept of an EACMS into an EACS and EAMS creates lower BES security, as monitoring of industrial control system networks is not being integrated with monitoring of business networks, sensor networks, and other networks. A particular pain point is that EACMS requirements prevent outsourcing 24x7 network monitoring that includes systems or networks in CIP scope. The financial and human resources needed to apply EACMS compliance levels to monitoring (not controlling) are unnecessary.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Dennis Sismaet - Northern California Power Agency - 6	

Answer	No
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response: 1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy does not agree the modifications are cost effective at this time. This is based on the current effort to implement CIP-013-1, CIP-005-6, and CIP-010-3 has not been completed and therefore a full understanding of the current costs is not known to establish a baseline with which to measure against. Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools in the required time period. Also, Duke Energy has yet to evaluate the impacts of defining and implementing EACMS and PACS related controls to meet this requirement.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
We do not feel that the level of administration and additional work is not cost effective for small organizations with limited resources. We recommend that exceptions are made for smaller entities that are more limited in their ability to get competative bids, and services to meet the intent of the FERC directives.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Scott Tomashefsky - Northern California Power Agency - 4	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the FERC directives can be executed in a cost-effective manner. There will be an undue cost and burden initially to conduct business another way by adding EACMS and PACS to CIP-005 R3.1 and R3.2. Other costs will include providing new technology if not already present to track, store, and recall the data addressing the assessments provided by CIP vendors.	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	

No comments.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Peter Brown - Invenergy LLC - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	

ITC is Abstaining	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) does not have a position nor comments in response to Question 6.	

Likes 0	
Dislikes 0	
Response	
Thank you.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

The addition of EACMs and PACs to the CIP-005 requirement 3 adds significant compliance efforts and costs to responsible entities. Entities that use vendors to assist in access monitoring, electronic or physical, for monitoring and threat hunting is a good thing. The more eyes on potential nefarious activity provides for a safer and more reliable grid.

Efforts like this sound good but do nothing to add to the cyber security of the grid.

Using the measure cited in part 3.1 as an example "Methods for monitoring activity (e.g. connection tables or **rule hit counters in a firewall**, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions" are now standard in most firewalls and can be provided as a print out for evidence. This however does nothing to secure the grid. The standards should address alerting on and actions taken on a unrecognized connections by an outside source. This would be more in line with providing cyber security, automated processes that transmit logs to SEIMS monitored by outside vendors is better for security. These types of issues should be addressed in CIP-013 requirement 1 already addresses connections inbound and outbound to assets.

Continual changes to standards and parts, even the slightest language and word changes cost budgetary dollars to review, comprehend, perform impact analysis, implement, test and meet at audit. The ambiguity around what “access” is, what “remote” is, and what “vendor” is in combination with the broad spectrum of interpretations by stringing these terms together creates a level of confusion that reduces cost effectiveness and efficiency. In the past, Standards Drafting Teams appear to work in silos from each other resulting in bleed over language which is similar or the same result.

Additionally, the continued absence of a provision for emergencies in CIP-013 R1 forces a Registered Entity to choose between compliance and reliability, and that very condition puts reliability at risk and creates costly undue compliance overhead. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is not cost effective for industry to allocate our limited resources to unnecessary compliance overhead when doing the right thing in crisis. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively manage the "knowns" and effectively mitigate the risk of the "unknowns". The simple inclusion of something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response:	
Thank you for your comment. Please see the SDT response at the beginning of question 6. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment	

Likes 0	
Dislikes 0	
Response	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT response at the beginning of question 6.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
NO. See response to question 7.	
Likes 0	
Dislikes 0	
Response	

7. Provide any additional comments for the standard drafting team to consider, if desired.	
Calvin Wheatley - Wabash Valley Power Association - 1,3	
Answer	
Document Name	
Comment	
Wabash Valley Power Alliance supports the comments submitted by NRECA. We individually comment that the low impact category has highly varied risk levels. This is especially true when a single access point controls access to a large number of BES assets. It is essential to impose BES Reliability standard on those systems whose architecture has a potential broad scale affect on reliability, while not adding excessive burden and costs on systems that are architected to have a minimal effect on grid reliability. Appropriate risk assessment by the SDT to focus efforts on those systems that will have an affect on grid reliability should be included as a component of the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT was unable to locate NRECA comments. After reading the comments above, it appears this comment may be for a different standards project.	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending an inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provide a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed though the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent out for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	
Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline

within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	
Document Name	
Comment	
AZPS requests more information be provided regarding the rationale for leaving the "system-to-system remote access" and "Interactive Remote Access" language in the Measures section of CIP-005-7 R3.1 and R3.2, after removing the language from the requirements. AZPS notes that the Measures section for CIP-005-7 R3.2 still references disabling remote access versus terminating remote access sessions. AZPS recommends that the SDT revise the Measures to maintain consistency with the requirement language. Similarly, AZPS recommends revising the language in CIP-013-2 R1.2.6 to maintain consistency with the language in CIP-005-7 R3.1 and R3.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT's original intention was to mirror language found in the FERC Order. The SDT received several comments about confusion caused by these terms when relating them to EACMS and PACS. The SDT considered this unintended consequence, and to address industry concerns is proposing alternative language that no longer requires reference to these terms and undefined phrases. The SDT also considered feedback about consistency and has adjusted the measures to align with the proposed language of the draft.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

Within CIP-010-4 Requirement 1 Part 1.6, PCAs should also be included in the Applicable Systems. When BES Cyber Systems and PCAs are located within the same ESP and software is validated and verified for the BCS but not the PCAs, a mixed-trust security environment is created within an ESP. The CIP-005-7 Implementation Guide for R3 uses the term "periodic" in every example of internal controls – with no definition or assistance regarding how long "periodic" is.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. PCAs are not within scope for this SAR.	
Erick Barrios - New York Power Authority - 6	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

This project should be canceled or at least placed on hold until the following occur:

1. DOE issues their report detailing how they will proceed with BPS Supply Chain requirements in accordance with the 2020 Presidential Executive Order. It is not prudent for NERC to continue spending inordinate amount of valued Industry stakeholders' time on this endeavor which will likely change in the near future as a result of DOE's efforts. Regardless, FERC will probably immediately order project changes anyway, even if Industry approves the proposal as is.

2. NERC provides a cost proposal, first and that it be accurate and reasonable. Future SARs should not be allowed through the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting and deserve to know the cost of what they are voting on.

3. FERC levels the playing field by ordering BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs. NERC's response to SAR page three Market Principle one was inaccurate. California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs. This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs. Additionally, this results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs like NCPA.

4. Finally, future submittals/proposals should not be sent for balloting until the CIP SDT not only develops proposed standard revisions, but also develop guidance and audit approach measures, that Auditors shall be required to follow, which should be balloted/commented on at the same time as the proposed standard revisions. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

Likes 0	

Dislikes 0	

Response

1. The standard drafting team recognizes that there may be future regulations issued as a result of the Executive Order regarding Bulk-Power System security. However, at this time the standard drafting team does not believe there is an indication that future regulations would be incompatible with the CIP supply chain requirements. Moreover, FERC has not adjusted the deadline for meeting the directive. As such, the standard drafting team will continue work on revising the CIP supply chain requirements to meet the regulatory deadline within the FERC Order. If an Entity is concerned about issues created from Executive Orders, DOE updates to documents, or FERC orders there are many avenues to make comment and affect change. Entities are free to comment directly to those organizations or work with trade groups (for example EEI or NATF) to craft comments as a group. Both of those options are open within the posted comment periods.

2. The standard drafting team posted the SAR for comment, and the SAR was vetted through the Standards Committee. Throughout this process, entities have the opportunity to indicate if the proposed scope will result in cost impacts that outweigh the benefit of the standard. The standard drafting team did not receive a majority of comments on the SAR that the cost of implementing these revisions outweighed the security benefit. As such, the standard drafting team will continue drafting the revisions.

3. As noted above, the standard drafting team has a regulatory deadline and cannot halt development at this time to accommodate any FERC activity regarding tariffs. Furthermore, the standard drafting team asserts that the proposed revisions as drafted do not preclude any market solutions to achieving compliance with that standard.

4. Finally, developing audit approaches is not within the scope of a standard drafting team's work. However, industry is provided with an opportunity to submit comments on the Reliability Standards Audit Worksheets (RSAWs) once developed.

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Support SDT consideration of formally defining "vendor" in the NERC Glossary of Terms. With the supply chain CIP-013-2, suggest inclusion of PACS peripherals (badge readers).

There are significant risks associated with PACS peripherals.

When contactless smart cards are implemented and deployed properly, they represent one of the most secure identification technologies available. However, some manufacturers, in an attempt to sell a 'universal' reader capable of reading almost any contactless smart card technology, actually disable the built-in security mechanisms. These readers, referred to as 'CSN readers', only read the card's serial number which, per ISO standards, is not be protected by any security. The ISO standard specifies use of the CSN for a process referred to as anti-collision, which is designed only to identify more than one distinct card in the field of the reader, and does not include security measures. An understanding of these details can allow a perpetrator to build a device to clone (or simulate) the CSN of a contactless smart card.

CSN refers to the unique card serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443and 15693. The CSN goes by many other names including UID (Unique ID), and CUID (Card Unique ID). It is important to note that the CSN can always be read without any security or authentication per ISO requirements.

Providers who seek to provide the lowest cost product, often choose not to pursue proper licensing of the security algorithms to minimize their costs. They also often fail to educate their customers on the compromise they are introducing into the customer's security solution. While the customer may benefit from a low price at install, the long term cost of a security compromise can be catastrophic. (Source - HID Global)

Emerging PACS technology includes IP Based Door Access and Entry Control Systems. This eliminates the need for a door controller. The built in intelligence system within the badge reader allows the access control decision to be made at the door controller in the event the network is down.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered feedback about defining the term "vendor" and decided not to create a formal glossary of terms definition to allow needed flexibility for each entity to document within their plan what constitutes a vendor. Instead,

the SDT has documented their intent regarding the use of this undefined term within the Technical Rationale for CIP-013-2; which reads, "The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." Regarding PACS peripherals, the SDT's inclusion of PACS in CIP-013-2 does not modify nor superseded the NERC Glossary of Terms definition and exclusions for PACS which states, "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." There is an appreciation that emerging technologies may change the manner within which certain technologies operate; however, due to the pervasive use of the term PACS, it is not within the scope of the 2019-03 SAR to modify this definition.

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments".

The changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following:

CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors, or vendors).

CIP-002 is a more appropriate choice for identifying and categorizing vendor systems that reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access – much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people). CIP-005, CIP-007, and CIP-010 already address controls for configurations, accounts, and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case, the justification would be "vendor remote access." These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Standard Drafting Teams (SDTs) have been in communication and continue to be in communication. After the teams reviewed the proposed EACMS split by project 2016-02, it was determined that this split is outside the scope of all three CIP SDTs (Project 2016-02 (CIP Virtualization), 2019-02 (CIP BCSI), and 2019-03 (Supply Chain)). A SAR will be drafted and submitted for future consideration. Any modifications made by project 2016-02, will be made following the completion of the 2019-03 project.	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to EEI.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
There are cases where the requirements would include “BES Cyber Systems, and their associated EACMS and PACS” as Applicable Systems (such as in CIP-010-4 Part 1.6, CIP-013-2 R1, R1.1, R1.2, R1.2.5). If associated PCAs are not included, the rest of the cyber assets within an	

Electronic Security Perimeter will be vulnerable. For example, PCA patches may be inadvertently loaded with Trojan Horses, malicious sniffers, etc., which may affect the rest of the devices in the network – including BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT appreciates the concerns raised and has not removed PCAs from the Applicable Systems of existing approved and future enforceable requirements; however, it is also not within the scope of the 2019-03 SAR to include PCAs in any new or modified requirements where PCAs do not already exist. The absence of PCAs does not preclude an entity from implementing processes that go above and beyond the minimum requirements of the Standard, and entity's may choose based on risk to include PCAs within their program.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Seattle City Light concurs with the comments provided by Snohomish PUD	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to Snohomish PUD.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	

Santee Cooper has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	
Document Name	
Comment	
Consistency across the three supply chain standards is of paramount importance. Please consider integrating consistent language into each standard, as applicable.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Thank you for your comment. The team reviewed to ensure language is consistent across the three Supply Chain standards. The SDT notes that while some words may be considered 'not consistent', it makes sense for the use within the appropriate requirement language.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	
Document Name	

Comment	
The clarification of vendor-initiated in CIP-005 R3 is valuable, but it doesn't solve the challenge of a contract employee (a vendor according to Supplemental Material sections of the Standards). A contract employee who initiates access to an applicable system remotely would be subject to these requirements, even if they are using Registered Entity owned and managed systems to initiate that access.	
Likes 0	
Dislikes 0	
Response	
The SDT considered feedback about defining the term "vendor" and decided not to create a formal glossary of terms definition to allow needed flexibility for each entity to document within their plan what constitutes a vendor, and believes there is sufficient detail within the Implementation Guidance and Technical Rationale for CIP-013-2 clarifying that it is up to the entity to define vendor. The SDT has documented their intent regarding the use of this undefined term within the Technical Rationale for CIP-013-2; which reads, "The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	
William Winters - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". R2 requires the responsible entity to	

implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
No additional comments on this question.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	
CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by	

controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22) CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	
Dislikes 0	

Response
The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS: 1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.", 2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and 3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks". In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to

protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.
The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.
Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."
While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.
Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through
a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.
The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore, the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.

Lastly, The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply

chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	

The continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational. ATC requests serious reconsideration and contemplation of language to fix this so we can effectively plan for the "knowns" while effectively mitigating the risk of the "unknowns" without a violation. The simple inclusion of

something like "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances". ATC believes it was the original SDT's intention for this to be a future-looking planning standard instead of a real-time/near real-time operating horizon standard, and does not believe it was the original drafting team's intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation. If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are "unplanned" and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Linn Oelker - PPL - Louisville Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
I support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	

Ginette Lacasse - Public Utility District No. 1 of Chelan County - 1, Group Name PUD #1 Chelan	
Answer	
Document Name	
Comment	

CHPD maintains that it does not agree with the inclusion of PACS in the scope of Project 2019-03. As stated in Cyber Security Supply Chain Risks Staff Report and Recommended Actions, "The potential risk of supply chain compromise described can be mitigated in part by controls, some of which are addressed it the CIP Reliability Standards while others can be addressed in entity policies and procedures … In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." (p. 14-15). CHPD agrees that PACS pose a lower risk to the BES than other classifications (BCA, EACMS, and PCA). PACS have no 15-minute BES impact and no access to BCS or ESP. CHPD believes that PACS should be excluded from Project 2019-03 for CIP-010 and CIP-013 due to their lower risk to the BES. CHPD instead recommends a best practice approach and adequate cyber security controls be applied to PACS for the same justification as to why they were applied to PCAs in the Cyber Security Supply Chain Risks Staff Report and Recommended Actions (May 17, 2019, p. 21-22)

CHPD requests coordination between Project 2016-02 and 2019-03 as changes of the EACMS classification continues to be developed.

Likes 0	
Dislikes 0	

Response

The SDT appreciates the thorough nature of comments raised regarding the inclusion of PACS. After extensive dialogue and consideration, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:
1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "Cyber Security Supply Chain Risks".

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "Cyber Security Supply Chain Risks", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES, and are implemented with that specific intention to protect the BES Cyber System, whereas PCAs are not. This supports the argument that the criticality of PACS and subsequent potential impact to reliability of the associated BES Cyber System is not equivalent to a PCA and should not be treated as such.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

Some comments received seem to be in alignment with NERC about the attenuated relationship between BES Cyber Systems and PACS in that NERC acknowledges on page 15 of their final report on "Cyber Security Supply Chain Risks" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access."

While it may be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor intentioned to gain unauthorized electronic access to a PACS does so with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance and further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Additionally, there is some precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through

a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT considered a potential parallel with BES Cyber Asset definitional qualifier, "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.", and the necessity of a secondary physical action subsequent to cyber-compromise of a PACS, the SDT asserts these are dissimilar concepts that cannot be compared. The concept excluding redundancy is intentioned to mean that if one Cyber Asset is compromised the likelihood that its counterpart is also compromised applies; therefore,

the assumption is made that both are compromised simultaneously to assure effective measures are applied to all BES Cyber Assets that contribute to reliable operation of the BES regardless of redundancy. While the constructs are dissimilar, if one were to entertain the parallel it could be reasoned that cyber-compromise of a PACS is a likely indicator that the secondary (or tertiary) action is imminent; therefore, the secondary (or tertiary) action must be a similarly assumed threat and predictable outcome and as a result not acceptable as a justification for lower risk.
The SDT must include EACMS in CIP-005-7 to meet FERC directives. In Order No. 850 the "supply chain risk management Reliability Standards" is a term that collectively refers to CIP-013-1, CIP-005-6, and CIP-010-3. Therefore, any directives which pertain to the supply chain risk management Reliability Standards pertain to the entire set of above listed Standards. Specifically, paragraph 1 describes the term at the outset of the Order No. 850:

"Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)."

Paragraph 5 of Order No. 850 is the first time instance of the directive:

"To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards…"

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

Southern would like, as with EEI, for the SDT to more clearly define how vendor remote access is to be addressed when a staff augmented contractor is essential to the reliable operations to the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services that include regular access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA.

Consider a proposal to modify the SAR to remove EACMS from the scope of CIP-005.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT's response to EEI.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
We appreciate the SDT efforts. Cyber Security is an ever changing issue and the Standard development process is just too slow for specifics. We believe entities should be required to regularly evaluate the risks and develop their own risk-based mehods of protection. This approach would allow entities to concentrate more on protecting the BES and less on complying with specific requirements that may or may not be adequate or cost effective. This approach would likely result in fewer findings of non-compliance and more recommendations for improvement, but provide more effective Critical Infrastructure Protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed CIP-013 and believes the requirements are written in a manner that allows this type of flexibility.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	

Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to MRO NSRF.	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to MRO NSRF.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	
These changes proposed have little to do with Supply Chain. When considering Supply Chain and vendors and their remote access, the SDT may must re-review the SAR and separate concepts with personnel and their authorizations from systems and their authorized purposes and capabilities. This can be achieved by minor changes in the following:	

CIP-004-6 already includes controls for authorizing personnel and is the appropriate standard area to authorize vendors. Consider authorization and access of personnel (no matter employees, contractors or vendors).

CIP-002 is a more appropriate choice for identifying and categorizing vendor systems which reside at an entity location. This allows an entity to use existing processes to identify vendor vs entity BCS and define and declare the purpose of the vendor system – i.e., providing vendor remote access – much as an entity identifies an EACMS or PACS purposes. This allows an entity to consider the capability and define what systems/cyber assets and software are authorized vs what they have not authorized (similar to how an entity authorizes people).

CIP-005, CIP-007 and CIP-010 already address controls for configurations, accounts and network/firewall rules) including identifying the protocols (RDP, SSH, etc..) ingress/egress to a BCS and a business justification in CIP-005. In this case the justification would be "vendor remote access."

These considerations use language and controls which separate and authorize people from authorizing systems and allows an entity to focus on defining the people, their authorizations and accounts (for vendors), and allows a focus on defining the purpose and function of a BCS, its configured apps and account privileges.

Secondly, the continued absence of a provision for emergencies in CIP-013 R1 creates a condition where a Registered Entity must choose between compliance and reliability, and that very condition puts reliability at risk. It is unreasonable to obligate a Registered Entity to put reliability at risk when in crisis, and then further punish an entity that does the right thing with a self-report if an after the fact supplier assessment must occur when faced with conditions like CIP Exceptional Circumstances. It is equally unreasonable for a Standard to become a distraction or dissuasion from doing the right thing. The NERC FAQ published Feb 18, 2020 clearly states the position that "CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements." For this to be a truly objective based Standard the requirement language should encourage "reliability and security" such that Registered Entities are permitted to develop a Supply Chain Risk Management Plan resulting in those outcomes without creating an automatic violation. CIP Exceptional Circumstances by their very nature are unplanned, yet the absence of these words creates a condition where the Registered Entity is facing noncompliance if not clairvoyant for a Requirement that was intended to be future-looking and not operational.

NERC should implement language to fix this so we can effectively plan for the "knowns" while effectively mitigating the risk of the "unknowns" without a violation. The simple inclusion for example of "1.3. Documented provisions for emergency procurements, including methods and timeframes to mitigate the risk of after the fact supplier risk assessments related to CIP Exceptional Circumstances". It was the original SDT's intention for this to be a future-looking planning standard team instead of a real-time/near real-time operating horizon standard, and was not NERC nor the original drafting team's intention to penalize Registered Entities when performing emergency procurements based on operational emergencies, yet the FAQ and the emerging guidance from our regulators would interpret this as a violation. If CIP Exceptional Circumstances was not considered, or omitted, by the original SDT due to past understanding that such emergencies are "unplanned" and therefore not subject to CIP-013-1, and the current SDT is aware of this unintended consequence and oversight, then the current SDT should be permitted to make that clarifying change under the existing SAR. A provision like this benefits reliability because now we are all thinking about this as a potentiality and could be better prepared to respond in crisis without having to choose between compliance and reliability. ATC appreciates the consideration.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. Please see the SDT's response to MRO's comments.

Denise Sanchez - Denise Sanchez On Behalf of: Glen Allegranza, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	
Document Name	

Comment
N/A

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 6, 5, 3; Derek Brown, Westar Energy, 1, 6, 5, 3; James McBee, Westar Energy, 1, 6, 5, 3; Marcus Moor, Westar Energy, 1, 6, 5, 3; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Evergy (Westar Energy and Kanas City Power & Light Co.) incorporate by reference the Edison Electric Institute's response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI Q7.	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Puget Sound Energy supporte the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	
Request that NERC notifies the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that the industry wants to provide feedback on the corrected, up-to-date documents. In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cybersecurity risk management controls ". R2 requires the responsible entity to implement its supply chain cybersecurity risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Your request has been passed along to NERC staff for consideration. In addition, supporting documents are located on the project. In addition, the noted modifications to the CIP-013-2 technical rationale have been updated.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES	

Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner's CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.	
Likes 0	
Dislikes 0	
Response	
Thanks for your comment. Please see the SDT's response to EEI.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Your request has been passed along to NERC staff for consideration.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI asks the SDT to more clearly define how vendor remote access is to be addressed when the service vendor is essential to the reliable operation of the BES. Proposed Reliability Standard CIP-005-7 does not provide a mechanism that exempts vendors who are providing essential contract services such as security access monitoring, logging and control through remote access to High and Medium Impact BES Cyber Systems, and associated EACMS, PACS and PCA. Presently, approved service vendors who require access to these systems are required to undergo personnel risk assessments through CIP-004-6, just as internal staff that needs similar access to these systems. Entity use of these services is often necessary to augment internal expertise or tools to perform these highly specialized duties necessary for the reliable operation of the BES or when project based work requires temporary vendor service providers to work on BES related equipment or software. The current draft of CIP-005-7, Requirement R3 does not distinguish between those service vendors who are properly vetted and those who are not authorized for remote access. For this reason, we are concerned that without an exemption for those service vendors that have already been vetted through the asset owner's CIP-004-6 process, many registered entities who safely and effectively use these services could be negatively impacted by the proposed Reliability Standard modifications. Among the services that could be impacted include the use of very specialized IT services needed to manage EACMS for BES Cyber Systems. To address this concern, EEI asks the SDT to consider scenarios where registered entities may use service vendors that would require vendor initiated remote access to EACMS for the purpose of enhancing or maintaining BES reliability and security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Modifications to CIP-004 are out of the scope of the 2019-03 SAR. The SDT considered this concern and determined there is sufficient detail within the Implementation Guidance and Technical Rationale for CIP-013-2 clarifying that it is up to the entity to define vendor. The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations	

with whom the registered entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." It is the SDT's intention for vendor to exclude staff augmentation or contracted resources that are an extension of the entity's employ and payroll.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI. In addition, CEC language is not within the team's scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC is Abstaining	
Likes 0	

Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MidAmerican supports EEI comments. MidAmerican also requests the standard drafting team consider adding language regarding CIP Exceptional Circumstances or other provisions for emergency procurements. The absence of such language could result in a Registered Entity having to choose between compliance and reliability in an emergency situation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to EEI. In addition, CEC language is not within the teams scope of work in the SAR and goes beyond the directive and the supply chain report recommendations.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
GSOC and GTC notes that the replacement of the term "determine" with the term "detect" in CIP-005-7, R2.4 (now 3.1) creates significant technical issues and may be infeasible. More specifically, the revision to the term "detect" pre-supposes a technical method to automatically delineate or differentiate vendor–initiated sessions from other active remote access sessions, which may be technically infeasible. In the previous version of the Guidelines and Technical Basis, a method to identify all types of remote access and an ability to	

terminate vendor sessions was considered appropriate. This distinction is important because methods for identifying active remote access sessions may be able to identify active sessions, but may not be able to differentiate those sessions that are vendor-initiated. Accordingly, once active sessions are identified, human or manual intervention may be necessary to hone in on those sessions that are vendor-initiated, e.g., through use of dedicated vendor identification numbers or access names. For these reasons, GSOC and GTC recommends that the SDT revert the proposed revisions to use the term "determine."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The terminology and conceptual change to a 3 part requirement: "Detect/Terminate/Disable". The word "Determine" is unusual usage and not aligned with typical cyber security terminology. The reason for a separate requirement in our proposed R3.3 is simple; terminating existing sessions does not prevent an attacker from spawning new sessions, and it is very easy to automate such requests. The requirement to "disable active vendor remote access" is crippled by the word "active" because it does not clearly express a need to disable future sessions which are by definition not "active". Combining the two requirements is parsimonious of words to the point of obscuring the objective. Without a means of denying new sessions, whether granularly or globally, an entity could find themselves playing "whack-a-mole" with an adversary and never able to manually keep it with automated requests. An example of granular control might be disabling a specific vendor's remote access account, blocking requests from a specific IP address or range, or changing an authentication token or password for a particular user account's remote access. This could be an absolute block or a suspension on new sessions for a timed period. For a global option, examples include simply denying all remote access attempts via change to a global VPN policy, firewall rule, etc. This is the proverbial "take a fire axe to the Internet connection" option.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
CPS Energy appreciates the standards drafting team efforts and supports mitigating risks to the BES in a cost effective manner across industry.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the SDT's response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to NPCC RSCC.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2019-03 Cyber Security Supply Chain Risks

Additional Ballot and Non-binding Poll Open through June 22, 2020

Now Available

The additional ballot and non-binding poll are open through **8 p.m. Eastern, Monday, June 22, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

The standard drafting team's considerations of the responses received from the last comment period are reflected in these drafts of the standards.

Balloting

Use the Standards Balloting and Commenting System (SBS) to submit votes. Contact Wendy Muller regarding issues using the SBS.

Note: Votes cast in the previous ballot will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to vote again in the additional ballot. NERC asks those not wanting to vote affirmative or negative cast an abstention to ensure a quorum is reached.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through June 22, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, June 22, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 12-22, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/198)
Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 2 ST
Voting Start Date: 6/12/2020 12:01:00 AM
Voting End Date: 6/22/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 237
Total Ballot Pool: 300
Quorum: 79
Quorum Established Date: 6/22/2020 5:20:06 PM
Weighted Segment Value: 34.44

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	14	0.25	42	0.75	0	6	18
Segment: 2	6	0.5	2	0.2	3	0.3	0	0	1
Segment: 3	67	1	15	0.319	32	0.681	0	6	14
Segment: 4	20	1	5	0.357	9	0.643	0	0	6
Segment: 5	70	1	20	0.351	37	0.649	0	2	11
Segment: 6	46	1	11	0.324	23	0.676	0	0	12
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	0	0	1	0.1	0	1	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	1	0	0	0	0	0	0	1	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	300	6.1	70	2.101	149	3.999	0	18	63

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		Abstain	N/A
1	Austin Energy	Thomas Standifur		Negative	Third-Party Comments
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Wes Wingen		Abstain	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Third-Party Comments
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	None	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Comments Submitted
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	sean erickson	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		None	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		Abstain	N/A
3	Austin Energy	W. Dwayne Preston		None	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
3	Great River Energy	Michael Brytowski		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	Comments Submitted
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	Aaron Smith		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Platte River Power Authority	Wade Kiess		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Comments Submitted
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		None	N/A
3	Seminole Electric Cooperative, Inc.	Michael Lee		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Westar Energy	Marcus Moor		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Jun Hua		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Scott Tomashefsky		None	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation - Black Hills Power	Don Stahl		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Cynthia Lee		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao	Helen Zhao	None	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NaturEner USA, LLC	Spencer Weiss		None	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OTP - Otter Tail Power Company	Brett Jacobs		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
5	Platte River Power Authority	Tyson Archie		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Comments Submitted
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	David Weber		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Westar Energy	Derek Brown		Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
6	Austin Energy	Andrew Gallo		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		None	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Colorado Springs Utilities	Melissa Brown		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Truong Le	Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Muscatine Power and Water	Nick Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Joel Robles		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		None	N/A
6	Westar Energy	James McBee		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green	Barry Jones	Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
8	David Kiguel	David Kiguel		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 300 of 300 entries

BALLOT RESULTS

Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 Non-binding Poll AB 2 NB
Voting Start Date: 6/12/2020 12:01:00 AM
Voting End Date: 6/22/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 217
Total Ballot Pool: 284
Quorum: 76.41
Quorum Established Date: 6/22/2020 6:06:39 PM
Weighted Segment Value: 33.14

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	73	1	10	0.233	33	0.767	13	17
Segment: 2	6	0.4	1	0.1	3	0.3	1	1
Segment: 3	66	1	13	0.333	26	0.667	12	15
Segment: 4	16	0.9	4	0.4	5	0.5	2	5
Segment: 5	68	1	17	0.37	29	0.63	9	13
Segment: 6	44	1	9	0.346	17	0.654	4	14
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	0	0	1	0.1	1	1
Segment: 9	1	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	2	1
Totals:	284	5.8	57	2.082	115	3.718	45	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Black Hills Corporation	Wes Wingen		Abstain	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Comments Submitted
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	None	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson	Barry Jones	None	N/A
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		Abstain	N/A
3	Austin Energy	W. Dwayne Preston		None	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
3	Great River Energy	Michael Brytowski		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza		None	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	Aaron Smith		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis		Abstain	N/A
3	Platte River Power Authority	Wade Kiess		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		None	N/A
3	Seminole Electric Cooperative, Inc.	Michael Lee		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Marcus Moor		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
4	CMS Energy - Consumers Energy Company	Aric Root		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation - Black Hills Power	Don Stahl		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Abstain	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Cynthia Lee		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NaturEner USA, LLC	Spencer Weiss		None	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	David Weber		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
5	Westar Energy	Derek Brown		Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
6	Austin Energy	Andrew Gallo		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		None	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Colorado Springs Utilities	Melissa Brown		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Truong Le	Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Muscatine Power and Water	Nick Burns		Negative	Comments Submitted
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Joel Robles		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		None	N/A
6	Westar Energy	James McBee		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green	Barry Jones	None	N/A
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 284 of 284 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standards for a formal 45-day comment and ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including Interactive Remote Access and system-to-system remote access) (2.5).	active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			or control the ability to reconnect for EACMS (3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~ third draft of the proposed standards for a formal 45-day comment and ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~May – June 2020~~
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems ~~and their associated: EACMS; PACS; and PCA~~ EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity ~~and their associated: EAMCS; PACS; and PCA~~	Have one or more method(s) ~~for detecting~~ to determine authenticated vendor-initiated remote connections ~~access sessions~~.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated ~~active~~ vendor-initiated remote ~~access~~ connections, ~~(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions),~~ such as: • Methods for accessing logged or monitoring information to ~~determine active~~ determine authenticated vendor-initiated remote connections ~~access sessions~~.; ~~• Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity~~

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			~~monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or~~ ~~Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.~~
3.2	EACMS and PACS associated with High Impact BES Cyber Systems ~~and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~ EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity ~~and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~	Have one or more method(s) to terminate ~~established~~ authenticated vendor-initiated remote ~~access~~ connections ~~sessions~~ and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to ~~disable~~ terminate ~~active~~ authenticated vendor-initiated remote ~~access~~ connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			physically disconnecting a network cable to prevent a reconnection. ~~(including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions), such as:~~ ~~PCA or BES Cyber System Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~PCA or BES Cyber System Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~ • ~~PACS or EACMS Methods to disable active vendor remote access either through Electronic Access Point, an Intermediate System or any other method of remote access~~

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including Interactive Remote Access and system-to-system remote access) (2.5).	active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method ~~for detecting~~to determine authenticated vendor-initiated remote ~~access sessions~~ connections for PACS ~~but had method(s) as required by Part 3.1 for other applicable systems types~~ (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate ~~established~~ authenticated vendor-initiated remote ~~access~~	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method ~~for detecting~~ to determine authenticated vendor-initiated remote ~~access sessions~~connections for ~~other applicable system(s) types~~EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3). ~~OR~~ ~~The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		connections ~~sessions~~ for PACS ~~but had method(s) as required by Part 3.2 for other applicable systems types~~ (3.2).	authenticated ~~established~~ vendor-initiated remote ~~access sessions~~connections or control the ability to reconnect for ~~other applicable system(s) types~~EACMS (3.2). ~~OR~~ ~~The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2)~~ ~~OR~~ ~~The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types.~~ ~~OR~~ ~~The Responsible Entity did not have method(s) as~~	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)~~	

D. Regional Variances

None.

E. Associated Documents

- ~~None.~~Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
45-day formal comment period with second additional ballot	July 28 – September 10 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7~~6~~

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7~~6~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002_5 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-76 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7~~6~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7~~6~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7~~6~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-76 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-76 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
			physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-7~~6~~ Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Ratioanle

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:
See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive-12 (HSPD-12), issued August 12, 2007.

.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1
Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~May – June 2020~~
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- ~~None.~~ Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1
Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~May – June 2020~~
45-day formal comment period with second additional ballot	July 28 – September 10, 2020
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated ~~(i)~~ remote access~~, and (ii) system-to-system remote access.~~.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all

applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all

applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-03 Cyber Security Supply Chain Risks

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-005-7, CIP-010-4, and CIP-013-2** by **8 p.m. Eastern, Thursday, September 10, 2020.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

Background Information

Project 2019-03 is in response to FERC Order 850 and the NERC Supply Chain Report to make modifications to the Supply Chain Standards, CIP-005-7, CIP-010-4, and CIP-013-2.

The NERC Supply Chain Report recommended including Electronic Access Control and Monitoring Systems (EACMS) that provide electronic access control and excluding monitoring and logging. The standard drafting team (SDT) considered excluding monitoring and logging. However, operationally classifying assets using multiple definitions under different requirements of the same standard, and from standard to standard, has the potential to create confusion and unnecessary complexity and administrative cost burdens in compliance programs.

The NERC Supply Chain Report recommended including Physical Access Control Systems (PACS) and excluding alerting and logging. The SDT considered excluding alerting and logging. However, operationally dealing with separate functionalities within the same asset definition has the potential to create confusion within the other standards that reference the current PACS definition in the applicability column.

In conclusion, the SDT decided to use the currently approved glossary definitions of EACMS and PACS in modifications to the Supply Chain Standards. The currently approved glossary definitions are all inclusive of the functionality of the systems and do not separate any subset of functions. Any modification to the existing definitions would have a wide impact on the CIP Standards outside of the Supply Chain Standards within scope of the 2019-03 SAR.

Questions

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

5. Provide any additional comments for the standard drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirements R1 and R2

The VRFs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirements R1 and R2

The VSLs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2

The VRFs for all requirements in CIP-013-2 did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirements R1 and R2

The VSLs did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirements.

VSL Justification for CIP-013-2, Requirement R3

The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to authenticate vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate established vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method for detecting vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
		method to terminate authenticated vendor-initiated remote connections for EACMS (3.2).	

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium for Requirement R3, which addresses Vendor Remote Access Management for EACMS and PACS, is consistent with Reliability Standard CIP-005-7 Requirement R2, which addresses Remote Access Management and includes requirements for vendor access management for high and certain medium impact BES Cyber Systems and associated PCA.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser-risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirements R1 and R2

The VRFs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirements R1 and R2

The VSLs did not change from the FERC-approved CIP-005-6 Reliability Standard.

~~**VRF Justification for CIP-005-7, Requirement R2**~~

~~The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.~~

~~**VSL Justification for CIP-005-7, Requirement R2**~~

~~The VSL is explained in the following pages.~~

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2~~, Requirement R1~~

The VRFs for all requirements in CIP-013-2 did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirements R1 and R2

The VSLs did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirements.

~~**VRF Justification for CIP-013-2, Requirement R2**~~

~~The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.~~

~~**VSL Justification for CIP-013-2, Requirement R2**~~

~~The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.~~

~~**VRF Justification for CIP-013-2, Requirement R3**~~

~~The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.~~

VSL Justification for CIP-013-2, Requirement R3

The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

~~VSLs for CIP-005-7, Requirement R2~~			
~~Lower~~	~~Moderate~~	~~High~~	~~Severe~~
~~The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.~~	~~The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.~~	~~The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.~~ ~~.~~	~~The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;~~

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from the FERC approved CIP-005-6 Reliability Standard, with the following exceptions. In the high and severe VSL, the second levels are removed because Requirement R2 Part 2.4 and Part 2.5 have been removed from the standard language. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

~~VSL Justifications for CIP-005-7, Requirement R2~~	
~~**FERC VSL G3**~~ ~~Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement~~	~~The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.~~
~~**FERC VSL G4**~~ ~~Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations~~	~~Each VSL is based on a single violation and not cumulative violations.~~

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management* for EACMS and PACS. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method ~~for detecting~~to authenticate vendor-initiated remote ~~access sessions~~connections for PACS ~~but had method(s) as required by Part 3.1 for other applicable systems types~~ (3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method for detecting vendor-initiated remote ~~access~~	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
	The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate established vendor-initiated remote ~~access sessions~~connections for PACS ~~but had method(s) as required by Part 3.2 for other applicable systems types~~ (3.2).	~~sessions~~connections for ~~other applicable system(s) types~~EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate ~~established~~ authenticated vendor-initiated remote ~~access sessions~~connections for ~~other applicable system(s) types~~EACMS (3.2). ~~OR~~ ~~The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2)~~ ~~OR~~ ~~The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types.~~	~~OR~~ ~~The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).~~

VSLs for CIP-005-7, Requirement R3			
Lower	Moderate	High	Severe
		~~OR~~ ~~The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)~~	

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	~~The proposed VSLs are based on the newly formed CIP-005-7 Requirement R3 which are modified from CIP-005-6 Requirement R2 Part 2.4 and Part 2.5. The Requirement R3 were modelled after the original CIP-005-6 Requirement R2 VSL's with the addition of PACS as an applicable system at a lower level than the other applicable system types listed in Requirement R3 Part 3.1 and Part 3.2.~~The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2~~ which Requirement R3 is modified from~~.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium for Requirement R3, which addresses Vendor Remote Access Management for EACMS and PACS, is consistent with Reliability Standard CIP-005-7 Requirement ~~R3~~R2, which addresses Remote Access Management and includes requirements for vendor access management for high and certain medium impact BES Cyber Systems and associated PCA.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser-risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system. These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements. Proposed Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 in CIP-005-6, and include modifications from the language used in CIP-005-6.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-7 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the third posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7.

To address industry concern during the second ballot regarding the required use of Intermediate Systems and EACMS, and the creation of a 'hall of mirrors', the SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems.

To further address this concern, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. To further address industry concern, references to Interactive Remote Access (IRA) and the undefined term system to system were removed.

The first table shows the current approved CIP-005-6 as compared to the current posting of CIP-005-7.

Current approved CIP-005-6 Language	**CIP-005-7 Language – Current Posting**
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
	Requirement R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS.* [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
	Requirement R3, Part 3.1: Have one or more method(s) to determine authenticated vendor-initiated remote connections.
	Requirement R3, Part 3.2: Have one or more method(s) to terminate authenticated vendor-initiated remote connections sessions and control the ability to reconnect.

This second table shows the last posted draft as compared to the current posting of CIP-005-7.

This illustrates Requirement R2, Part 2.4 and Part 2.5, which had been moved to R3 in the last posting, are back in R2 restoring CIP-005-6 and its Applicable Systems to the current approved language: High impact BES Cyber Systems and their associated to PCAs, and Medium impact BES Cyber Systems with External Routable Connectivity and their associated to PCAs.

This also demonstrates Requirement R3 has been modified to focus solely on EACMS and PACS associated to high impact BES Cyber Systems, and EACMS and PACS associated to medium impact BES Cyber Systems with External Routable Connectivity. The language of Requirement R3, Part 3.1 and Part 3.2 have been modified to 1) remove 'access' to address double jeopardy concerns with CIP-004-6; 2) replace 'detecting' with 'authenticate' to address concerns about real-time monitoring of vendor activity; and 3) replace 'sessions' with 'connections' to address industry concerns about ambiguity with the term 'session'.

CIP-005-7 Language – Last Posted second draft	**CIP-005-7 Language – redline from Last Posted**
	Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
	Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
Requirement R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*	Requirement R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
Requirement R3, Part 3.1: Have one or more methods for detecting vendor-initiated remote access sessions.	Requirement R3, Part 3.1: Have one or more methods to determine authenticated ~~for detecting~~ vendor-initiated remote connections~~access sessions~~.
Requirement R3, Part 3.2: Have one or more method(s) to terminate established vendor-initiated remote access sessions.	Requirement R3, Part 3.2: Have one or more method(s) to terminate authenticated~~established~~ vendor-initiated remote connections~~access sessions~~ and control the ability to reconnect.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-4 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the third posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-010-4.

To address the FERC directives, EACMS and PACS were added to the Applicable Systems for Requirement R1 Part 1.6. No modifications have been made to the requirement language itself.

The first table shows the current approved CIP-010-3 as compared to the current posting of CIP-010-4.

Current approved CIP-010-3 Language	CIP-010-4 Language – Current Posting
Requirement R1 Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	**Requirement R1 Part 1.6:** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

This second table shows the last posted draft as compared to the current posting of CIP-010-4.

CIP-010-3 Language – Last Posted second draft	CIP-010-4 Language – Current Posting
Requirement R1 Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	**Requirement R1 Part 1.6:** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-013-2 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the third posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-013-2.

To address the FERC directives, EACMS and PACS were added to Requirements R1 and R2.

The first table shows the current approved CIP-013-1 as compared to the current posting of CIP-013-2.

Current approved CIP-013-1 Language	CIP-013-2 Language – Current Posting
Requirement R1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*	**Requirement R1:** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
Requirement R1.1: One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	**Requirement R1.1:** One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
Requirement R1.2: One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:	**Requirement R1.2:** One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:
Requirement R1.2.5: Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	**Requirement R1.2.5:** Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and
Requirement R1.2.6: Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	**Requirement R1.2.6:** Coordination of controls for (i) vendor-initiated ~~Interactive R~~remote ~~A~~access~~, and (ii) system-to-system remote access with a vendor(s)~~.

This second table shows the last posted draft as compared to the current posting of CIP-013-2.

To address industry concern during the second ballot regarding 'hall of mirrors' for EACMS and the required use of Intermediate Systems, as well as concerns about inconsistencies in language between procurement planning requirements in CIP-013-2 and the operational security requirements of CIP-005-7, references to Interactive Remote Access (IRA) and the undefined term system to system were removed from, CIP-013-2 Requirement R1.2.6, because authenticated remote connections and system to system remote connections for EACMS and PACS; and IRA and system to system access to BCS and PCAs are all sub-types of vendor-initiated remote access.

CIP-013-1 Language – Last Posted second draft	CIP-013-2 Language – Current Posting
Requirement R1.2.6: Coordination of controls for (i) vendor-initiated remote access, and (ii) system-to-system remote access with a vendor(s).	**Requirement R1.2.6:** Coordination of controls for ~~(i)~~ vendor-initiated remote access~~, and (ii) system-to-system remote access with a vendor(s)~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

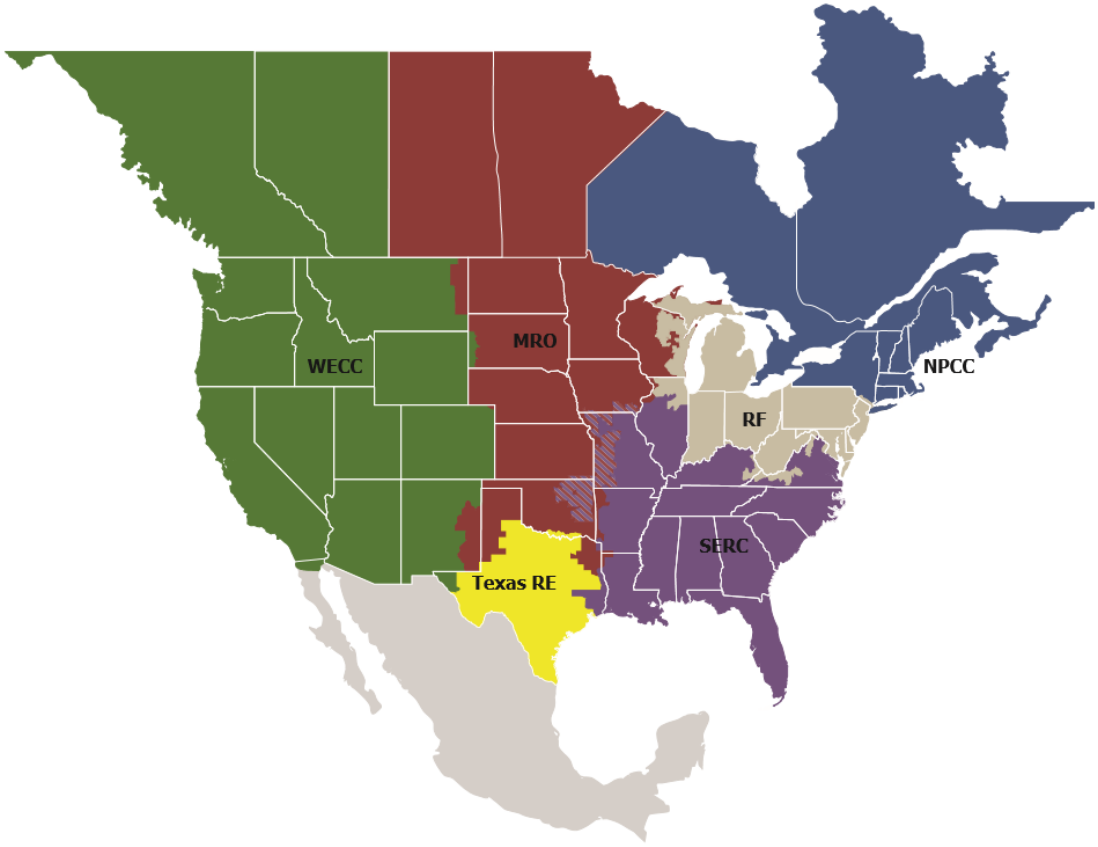
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[1].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:
See Secure Remote Access Reference Document (see remote access alert).

Rationale:
During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

~~May~~ July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

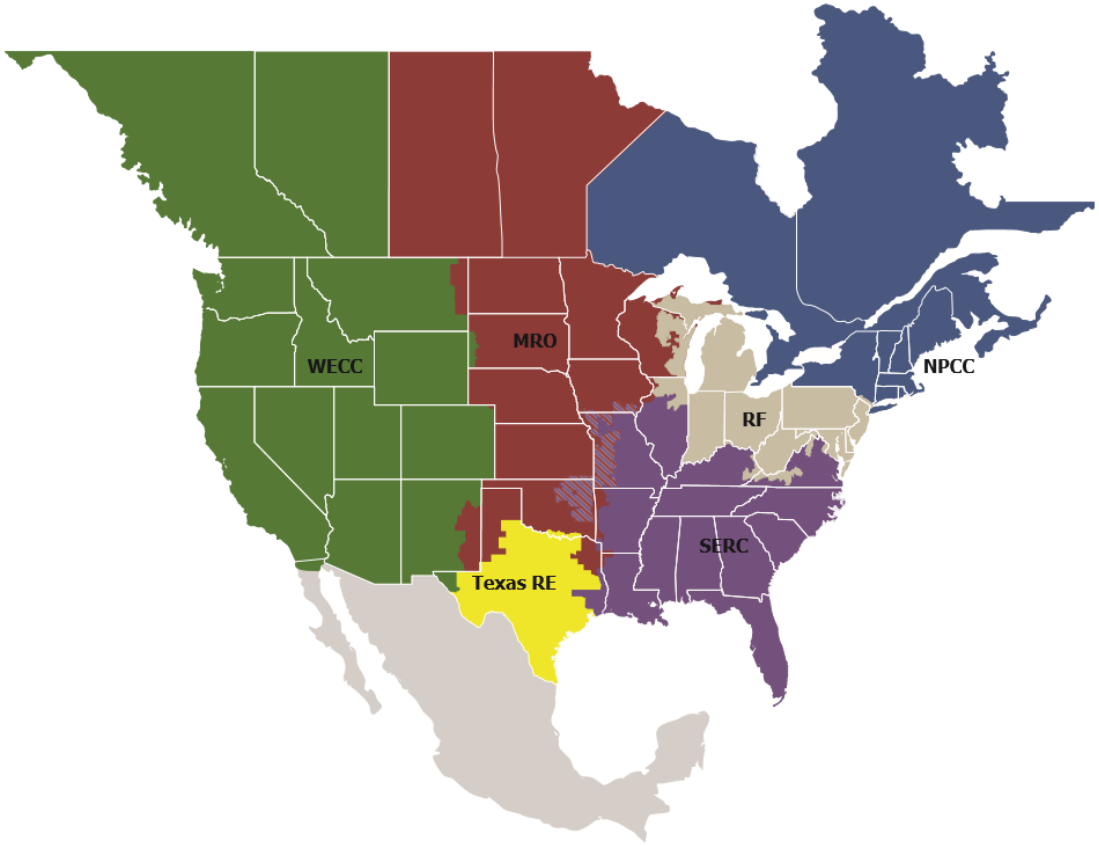
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). ~~Additionally, the SDT created Requirement R3 to specifically address added EACMS and PACS to the Applicable Systems for those requirements.~~ EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first ~~must first to~~ perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require ~~devices potentially require~~ physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[1].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting~~supporting~~ BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." ~~-~~While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. ~~With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.~~

~~Precedent is set in CIP-006-6 Requirement R1 Part 1.5 on the importance of PACS by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that a compromised PSP poses imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities.~~

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was ~~around~~ the risk associated with the ~~different aspects~~ access control vs. access monitoring functions of both EACMS and PACS. ~~—~~While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. ~~-~~The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS~~s~~), however if remote access is allowed, options to determine remote access connection(s)~~session(s)~~ and capability to disable remote access connection(s)~~session(s)~~ is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

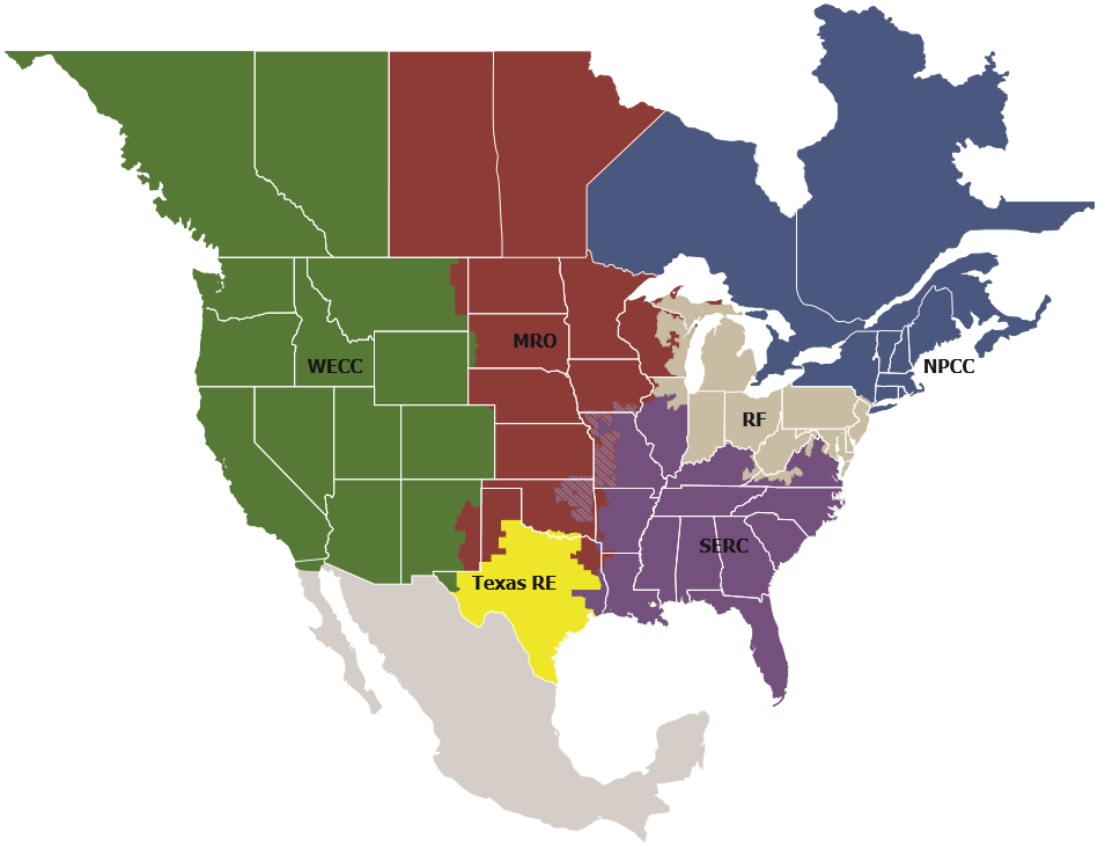
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rational for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

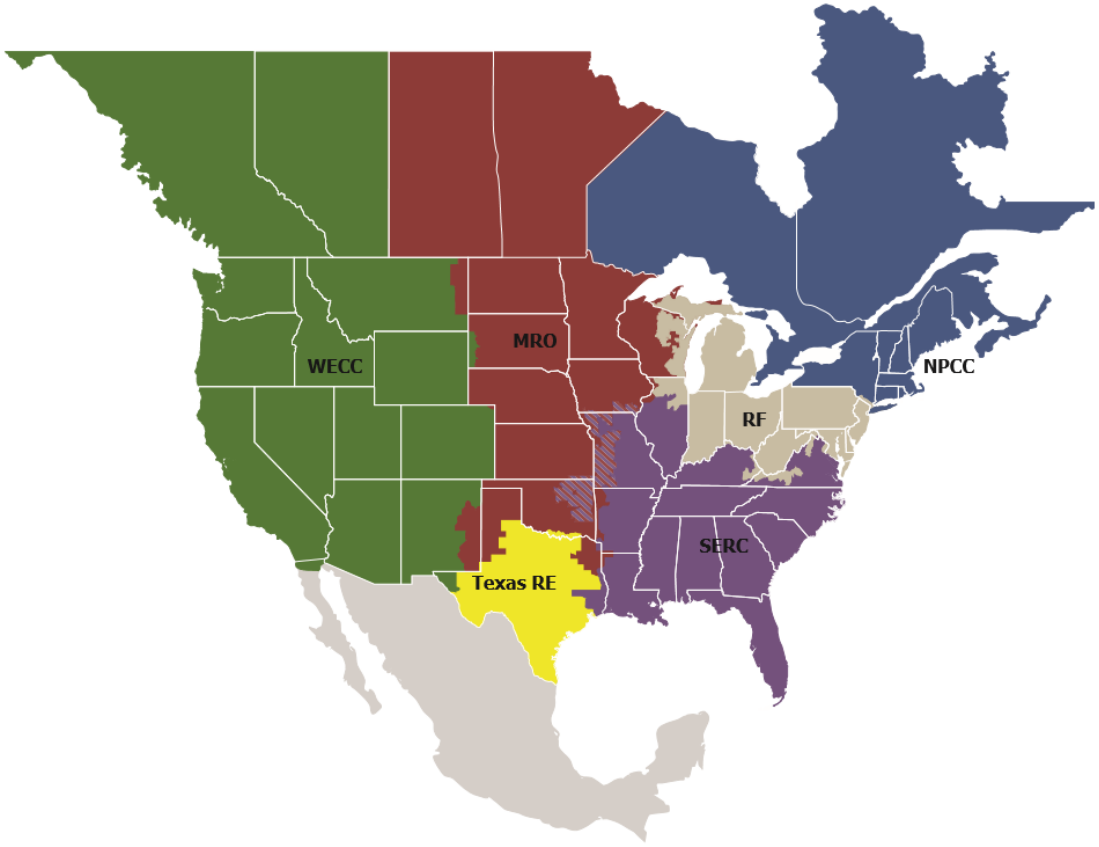
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rational for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

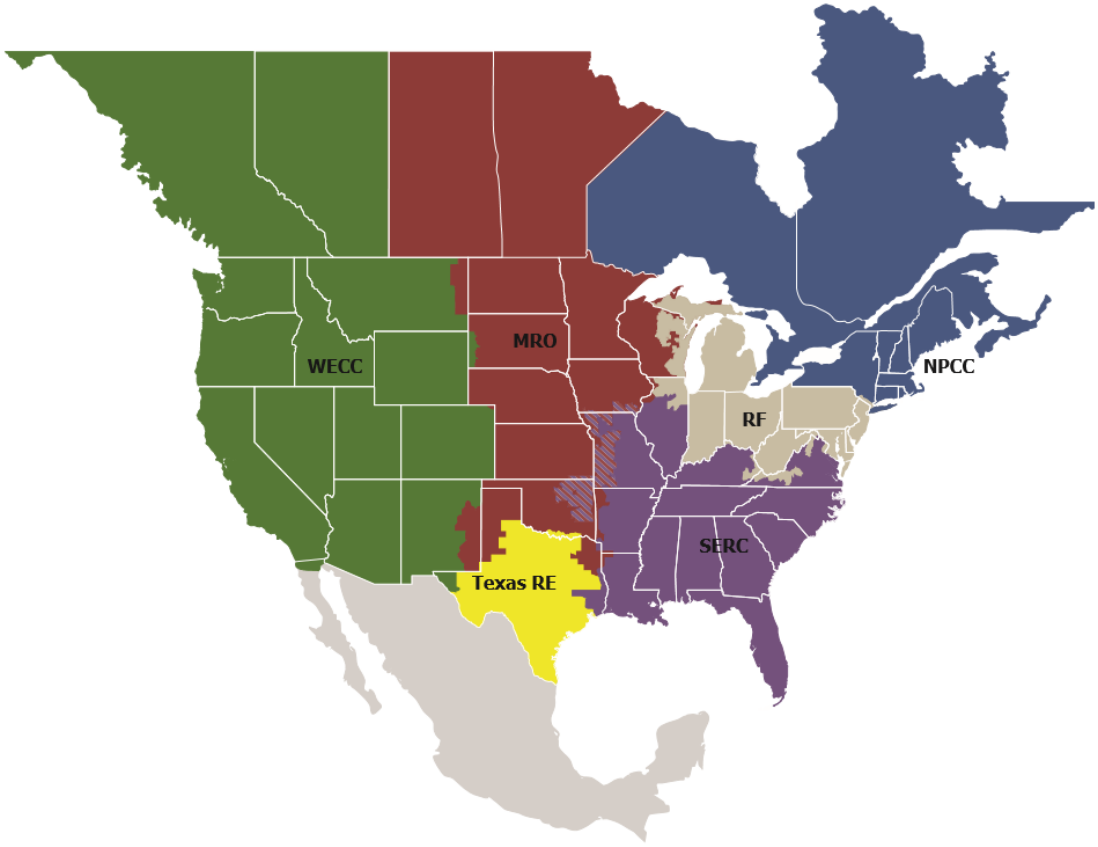
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

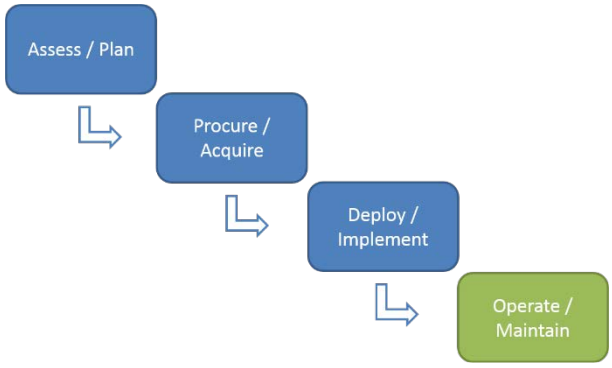
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

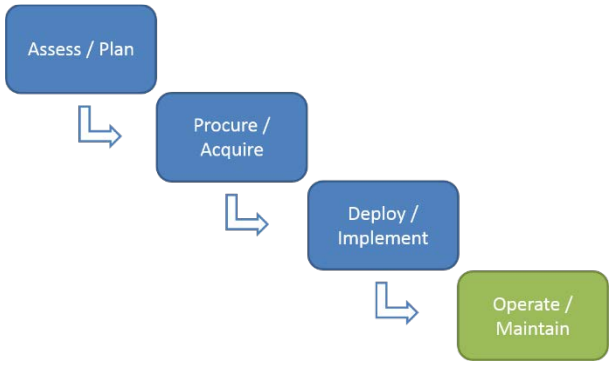
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

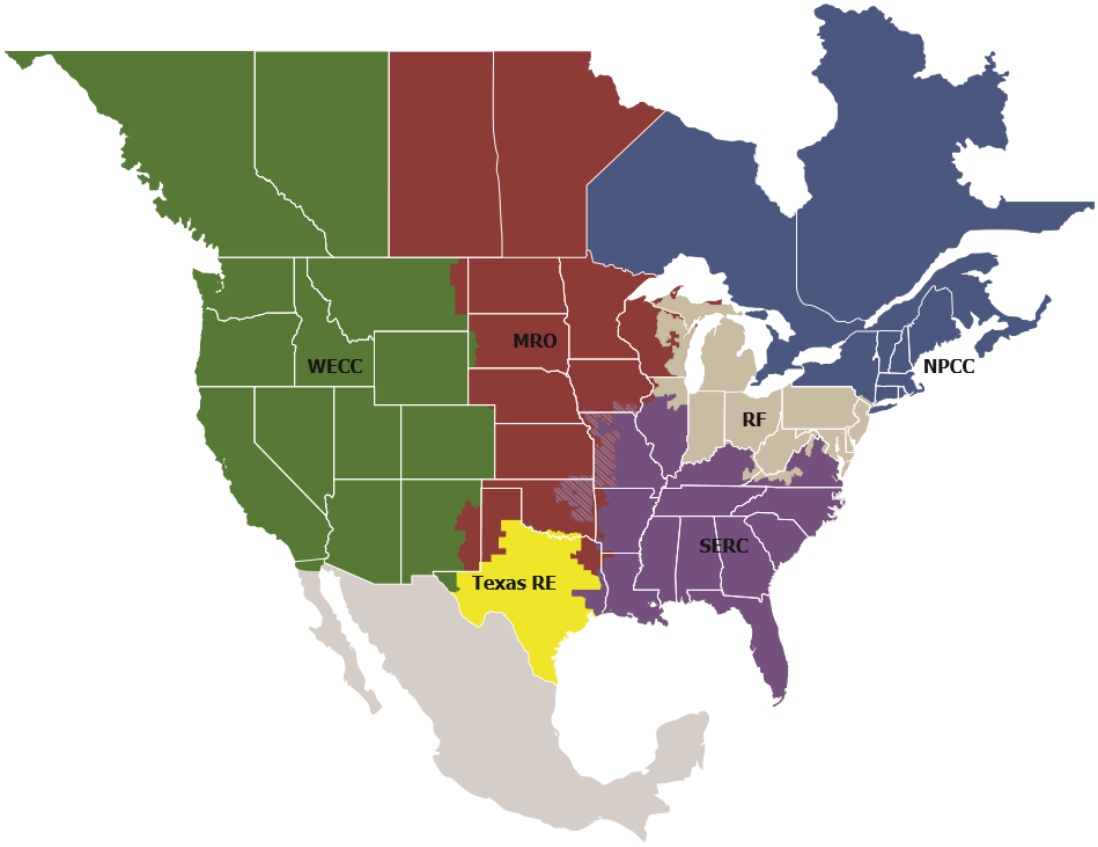
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*" [2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

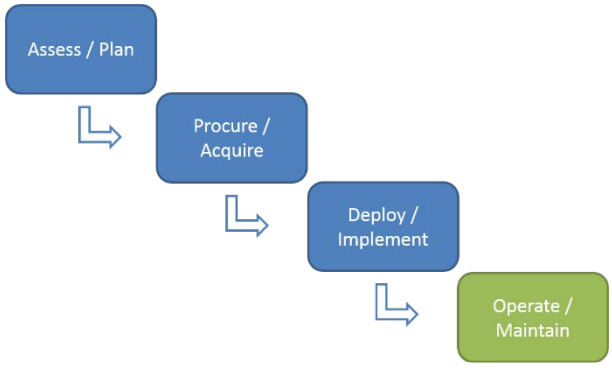
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement ~~R2~~R3

General Considerations for Requirement ~~R2~~R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

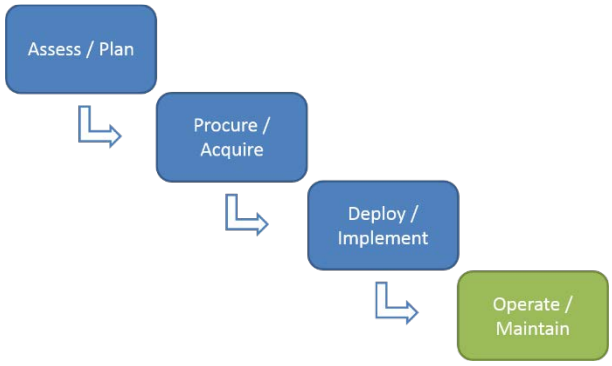
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

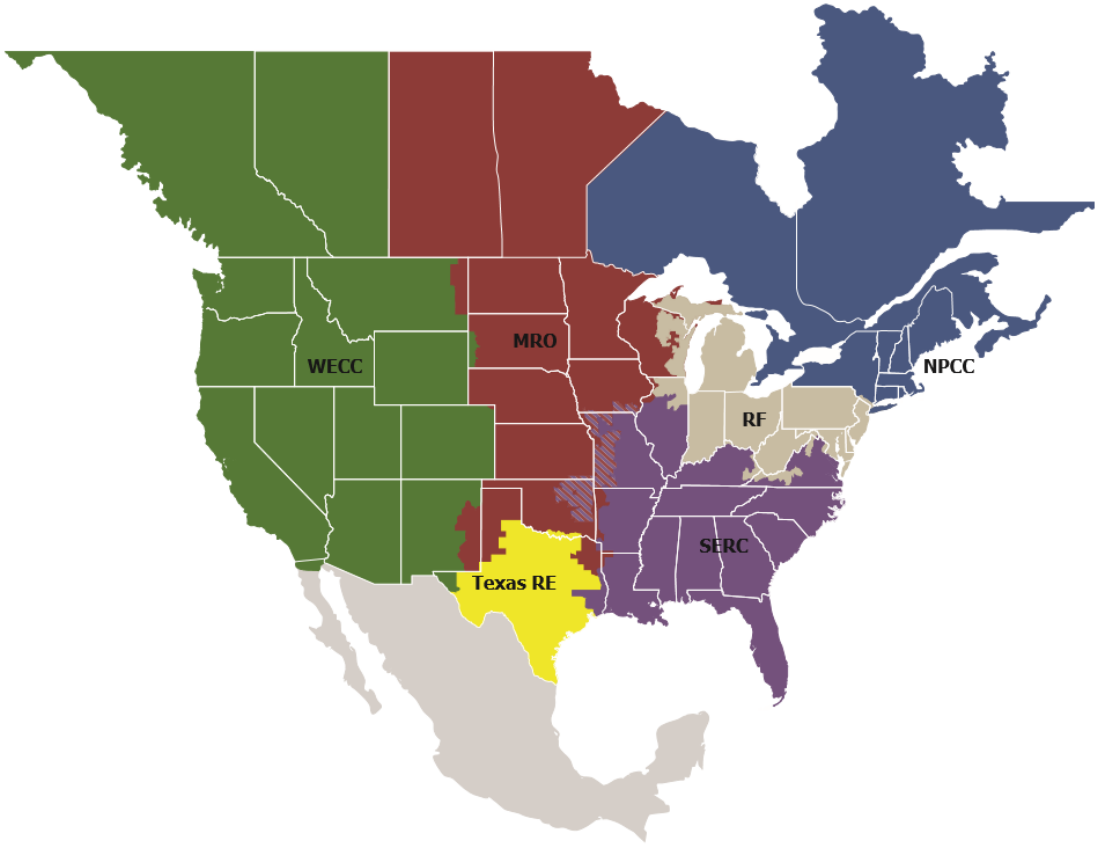
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements Parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method to determine authenticated vendor-initiated remote connections is documented and the ability to disable that remote connection is required. For example, if an entity utilizes its corporate remote access solution to allow remote connection into its PACS, the entity would need to document the authenticated remote connection method and develop a process to terminate such connections after authentication. Some examples of how an entity might terminate these connections may be as simple as, but are not limited to actions like disabling a token or certificate for a vendor account(s), suspending or deleting the vendor account(s) in Active Directory, blocking the vendor's IP range, or physically disconnecting a network cable.

Intermediate Systems (a subset of EACMS) use is not a requirement for remote access to other EACMS, lessening the potential of the recursive requirement ("hall of mirrors") However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS, the process of terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor attempts the remote access connection, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable the vendor's ability to make a connection. The remote access vendor will attempt to "connect" with the EACMS however, after unsuccessful authentication the connection attempt will be terminated. This scenario illustrates a method to disallow vendor-initiated remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes

to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

~~May~~ July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

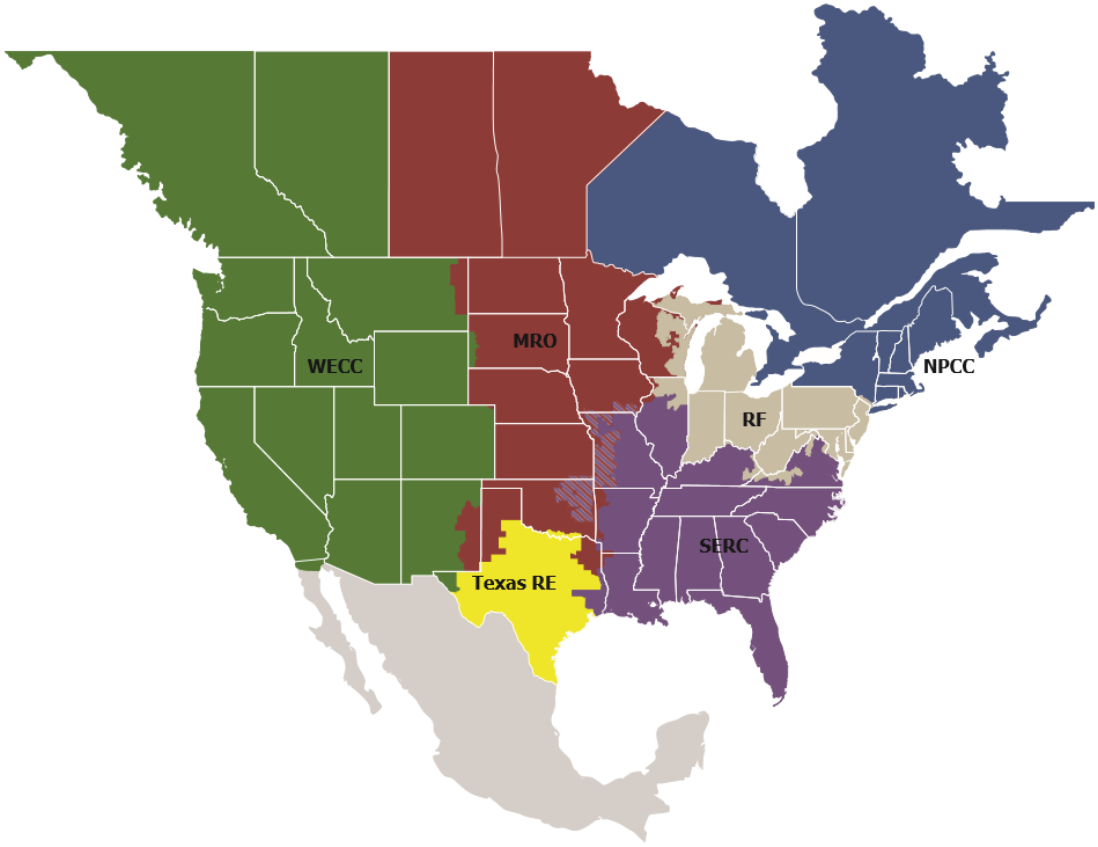
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements ~~along with adding EACMs and PACs to the Applicable Systems column for Requirement P~~parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. ~~-~~If an entity allows remote access to their EACMS and PACS the method to determine authenticated ~~for~~ vendor-initiated remote ~~access~~ connections ~~would be~~is documented and the ability to disable that remote ~~access~~ connection ~~would be~~is required. ~~-~~For example, if an entity utilizes its corporate remote access solution to allow remote ~~access~~ connection into its PACS, the entity would need to document the authenticated remote ~~access~~ connection ~~method, and~~method and develop a process to ~~remove~~ terminate such connections~~access~~ after authentication. ~~-Removing~~ Some examples of how an entity might terminate ~~access~~ these connections may be as simple as, but are not limited to actions like disabling a token or certificate for ~~that~~a vendor ~~user~~ account(s), ~~or~~ suspending or deleting ~~that user's~~the ~~-~~vendor account(s) in Active Directory ~~account~~, blocking the ~~IP~~ vendor's IP range, or physically disconnecting ~~pulling~~ a network cable.

~~Since~~ Intermediate Systems (a subset of EACM~~CSs~~) ~~are~~ use is not a requirement for remote access to other EACMS, ~~lessesning~~lessening the ~~s the~~ potential of the recursive requirement ~~-~~("hall of mirrors") ~~issue is lessened (see above examples for terminating remote vendor connections).~~ ~~-~~However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS, the process of ~~disabling remote access~~ terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. ~~becomes tricky. Since the standard requires the removal of remote access to EACMS how can that be accomplished on the EACMs itself, the "hall of mirror" effect?~~ For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor~~user~~ attempts the remote access connection~~session~~, the jump host will present both the Active Directory login screen as well as the multifactor access portal. ~~-~~The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable~~d~~ the vendor's~~user's~~ ability to make a connection. ~~"access" the EACMs.~~ The remote access vendor~~user~~ will attempt to "connect" with the EACMS~~s~~ however, after unsuccessful authentication the connection attempt ~~session~~ will be terminated.~~not allow "access" without the authentication methods being enabled, thus effectively not allowing remote access to that EACMS.~~ This scenario ~~shows~~ illustrates a method to ~~not~~ disallow vendor-initiated ~~-~~remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.

c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.

d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4~~3~~ Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4~~3~~ Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

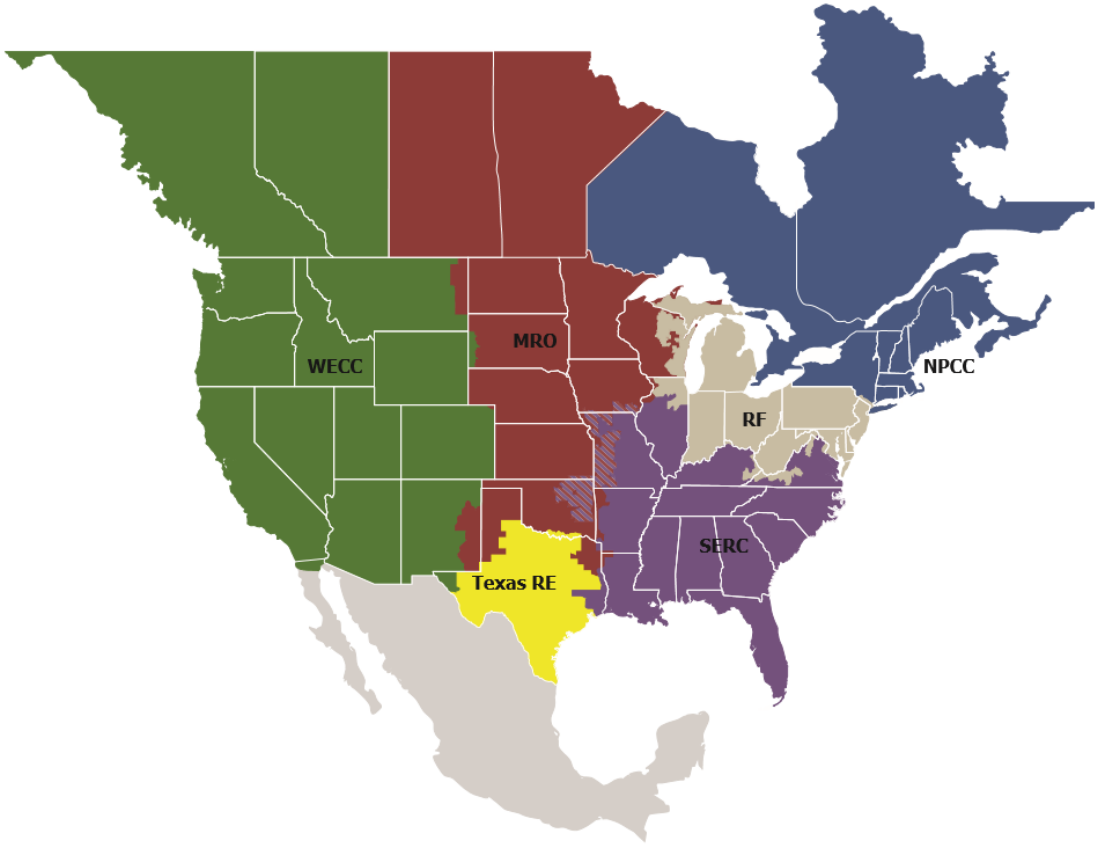
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Per Transient Cyber Asset Capability

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

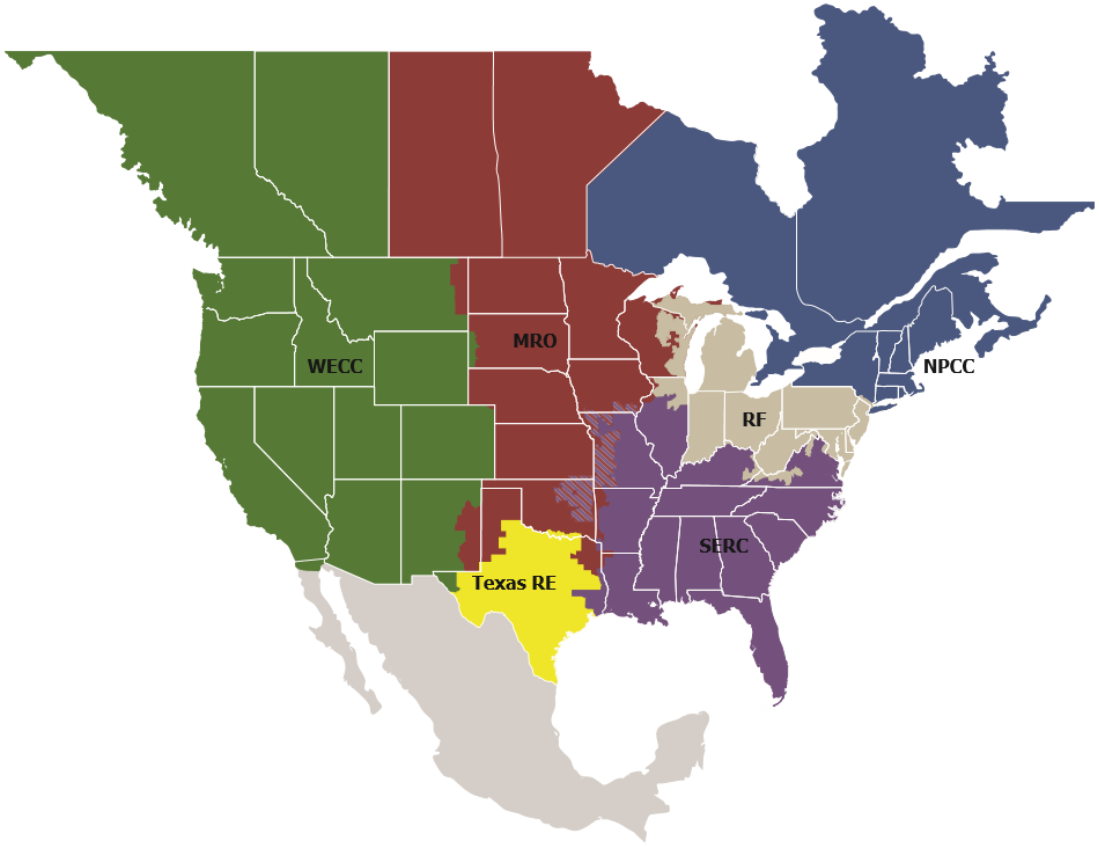
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Per Transient Cyber Asset Capability

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-2

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1] and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

1.2.6. *Coordination of controls for vendor-initiated remote access.*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-2.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the

following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2.

Requirement R3

R3. *Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-~~1~~ 2

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2~~1~~ – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1]~~.~~ and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2~~1~~ and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2~~1~~. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

1.2.6. *Coordination of controls for vendor-initiated remote access. ~~(i) vendor-initiated Interactive Remote Access, and (ii) system-~~ to-system remote access, as well as ~~Interactive Remote Access, which includes~~ with a vendor(s) initiated sessions.~~*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-~~1~~2.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4~~3~~, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems~~,~~ and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor*

products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:

- Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:
  - Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
  - Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.
- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access. ~~(i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access, as well as Interactive Remote Access, which includes with a vendor(s) initiated sessions.~~*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2~~1~~. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2~~1~~.

Requirement R3

R3. *Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through September 10, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Thursday, September 10, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

The standard drafting team's considerations of the responses received from the last comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **September 1-10, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify "Project 2019-03 Cyber Security Supply Chain Risks Observer List" in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2 (Draft 3)
Comment Period Start Date:	7/28/2020
Comment Period End Date:	9/10/2020
Associated Ballots:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 3 ST

There were 59 sets of responses, including comments from approximately 135 different people from approximately 85 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments for the standard drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Ali Miremadi	CAISO	2	WECC
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
CMS Energy - Consumers Energy Company	Jeanne Kurzynowski	3,4,5	RF	Consumers Energy Company	Jeanne Kurzynowski	Consumers Energy Company	1,3,4,5	RF
					Jim Anderson	Consumers Energy Company	1	RF
					Karl Blaszkowski	Consumers Energy Company	3	RF
					Theresa Martinez	Consumers Energy Company	4	RF

					David Greyerbiehl	Consumers Energy Company	5	RF
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy - FirstEnergy Corporation	4	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC

Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC

Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC

					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes there are several problems with proposed requirement R3 as presently written

- It addresses “authenticated vendor-initiated remote connections” without explicitly establishing a requirement for authentication, nor does it provide a working definition of a “remote connection.”
- Part 3.2’s mandate to control the ability of a vendor whose connection has been terminated to reconnect creates a consistency problem. There is no comparable requirement in Requirement R2 for vendor remote connections to BES Cyber Systems and PCAs.
- A second inconsistency is created by using the term, “remote connection” in R3, whereas the term, “remote access” is used in R2.

N&ST recommends the following changes:

- Move R3’s proposed Parts 3.1 and 3.2 to R2 and eliminate R3. N&ST sees no need to address vendor remote access to applicable systems in two separate, top-level requirements.
- Modify the “applicability” language in those two Parts to say, for example:
    - “EACMS and PACS:
    - associated with High Impact BES Cyber Systems, and
    - not located within any of the Responsible Entity’s Electronic Security Perimeter(s).”
        - NOTE: 2nd bullet is taken verbatim from the Glossary definition of IRA
- Add an explicit requirement to use at least one form of authentication.
- Consider adding language, taken from the existing IRA definition, that that clarifies "vendor remote access" originates from "Cyber Assets used or owned by vendors, contractors, or consultants." The SDT may want to consider adding this to existing R2 Parts 2.4 and 2.5, as well.
- Change “remote connection” to “remote access”
- The proposed requirement to control vendor reconnection should either be eliminated or added to existing R2 Part 2.5.

Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

ACES does not agree with the use of “authenticated” and “remote connections” in R3.

R3 without the word authenticated, covers all vendor connections .. CIP-004 R4.1 already requires access management for EACMS and PACS and CIP-007 R5.1 requires methods to enforce authentication. Further, as discussed on the project 2019-03 webinar, unauthenticated remote access is already addressed by the CIP standards. Lastly, an authorized remote connection can be made without being authenticated. Thus an authorized malicious insider could easily craft a denial of service without ever being completely authenticated. Removing the word “authenticated” would put more emphasis on **all** vendor connections and increases the security objective of R3. Suggested language:

“Have one or more method(s) to determine vendor initiated remote access.”

Secondly, the CIP standards have always used the NERC defined term: Interactive Remote Access and or remote access vs what is in the draft “remote connections”. ACES suggests using language consistent with existing standards. Without defining “remote connections”, it makes the requirement vague and could be interpreted differently. Suggested language:

“Have one or more method(s) to terminate vendor initiated remote access and control the ability to reconnect.”

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA proposes the SDT eliminate references to “vendor.” The requirements should apply to any active remote sessions.

Proposed change to R2.4:

Have one or more methods for determining detecting active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Proposed change to R2.5:

Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	
Comment	

Restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language is fine, but the language in R3 is unclear. It's not clear what "authenticated vendor-initiated" remote connections are. The intent seems clear, and the security necessity is warranted, but it is not clear why using something like "Have one or more method(s) for determining authorized vendor-initiated remote access connections" is not used. What value does using "authenticated" vendor-initiated remote access connections add? Why is "Remote Connections" used instead of "Remote Access" since R3 is "Vendor Remote Access"? What is considered a remote connection? Does a remote connection include both system to system communication and remote access? Is a remote connection from outside of an entities corporate network or is it a remote connection from inside an entities network but behind a firewall and using some remote access client?

Likes 0	
Dislikes 0	
Response	

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	
Comment	

If the requirements are technically the same, as it appears, then the new scope should be added to Parts 2.4 and 2.5. However, we believe the SDT was attempting to resolve some ambiguity that currently exists around what is vendor remote access. We commend the SDT for this effort, and request they clarify the existing requirements (parts 2.4 and 2.5). Specifically, vendor remote access should be defined or somehow clarified that it only includes access where the vendor's personnel or system has direct access and ability to control the session. Having IRA and system-to-system listed as examples, but not an all-inclusive list, would also be helpful.

Likes 0	
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	
Comment	

The SDT should provide guidance or clarify the role or function of Intermediate Systems in context of providing electronic access to EACMS and PACS located within an ESP vs outside an ESP.

If the SDT intends to *exclude* Interactive Remote Access (IRA) requirements for EACMS or PACS in CIP-005-7 R3.1 and R3.2, it should clarify that an intermediate system is not required to electronically access an EACMS and PACS located outside an ESP. However, if the EACMS or PACS is located within the ESP, the entity is required to utilize an Intermediate System for electronic access. This brings into scope all CIP-005 R2 requirements.

Without guidance, entities may interpret that an Intermediate System is never required for the vendor IRA to EACMS or PACS - even though they may exist within an ESP.

The SDT did not use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without the IRA requirements of CIP-005 R2?

The SDT could consider putting all vendor remote access sub-requirements in one requirement – 3.0.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

Agree with leaving R2 as is.

Disagree with need for a R3. Actually, the SDT should be providing us with a cost/benefit justification for change.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

We thought a CIP Modification SDT goal was to remove this language to assist the coming virtualization updates.

Request clarification on why CIP-005 R2 Parts 2.4 & 2.5 use the phrase “vendor remote access” while CIP-013 R1 Part 1.2.6 uses the phrase “vendor-initiated remote access” We are concerned that omitting “initiated” may introduce unintended requirements in CIP-005.

Likes 0	

Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC greatly appreciates the drafting team's efforts and thoughtful approach regarding this proposal. However, it is concerned that the splitting of these requirements creates significant potential for very different compliance obligations for the different classes of assets while attaining the same or similar cyber security protections as would be garnered solely with either set of requirements. More specifically, the differentiation between the requirements for PACS and EACMSs and the assets to which access is sought is likely to cause confusion as well as increase the potential for differing interpretations of compliance and "double jeopardy." That the proposed split of requirements would likely provide little or no additional security benefit, while being unduly burdensome for entities, creates additional concerns for responsible entities as they try to focus their resources on those activities that will have a net effect of enhancing security.

GSOC understands that industry comments have driven these proposed changes, and agrees that valid concerns have been presented (e.g., the hall of mirrors). In its response to question #2, GSOC proposes an approach to addressing these previous concerns and comments that will allow a return to a simpler approach for the requirements generally. We respectfully recommend that the SDT consider utilizing alternative approaches such as are proposed below, e.g., definition revision, to allow the requirements to more clearly and succinctly meet the Commission directives regarding EACMS and PACS. This simpler approach to address concerns will facilitate a reversion of the requirement language to the initial proposal where EACMSs and PACs were added as applicable systems for the existing requirements.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

please reference Marty Hostler, Northern California Power Agency, comments

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and adding R3 for EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We recommend that view only access by a vendor is not considered IRA, nor vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
To separate the remote access from the vendor remote access, FirstEnergy would respectfully suggest that the currently drafted R2 Parts 2.4 and 2.5 are reorganized to become R3 Parts 3.1 and 3.2. Subsequently, the currently drafted R3 3.1 and 3.2 become Parts 3.3 and 3.4.	
Likes 0	
Dislikes 0	
Response	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R2 Parts 2.4 and 2.5. However, ISO-NE recommends the use of consistent “vendor remote access” or “vendor-initiated remote connections” for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment
PG&E believes this is the appropriate modifications in-line with the industry comments made to the second Comment & Ballot. The restoration of the P2.4 and P2.5, along with the modifications made in Requirement R3 more clearly eliminate the potential interpretation that could have resulted in recursive requirements noted in Question 2 below.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	

Comment
MidAmerican supports EEI commnets

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment
Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	

Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy supports EEI's comments on Q1: "While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we ask the SDT to consider revising “vendor remote access” to “vendor initiated remote access” or provide clarification why they believe that all vendor remote access should be considered under Parts 2.4 and 2.5. EEI supports the current proposed draft language for Requirement R3." In addition, NVE supports the revision of "vendor remote access" to "vendor initiated remote access" due to current conflicting interpretations of P2.5 and 2.5 and CIP-005-6 by Regional Entities. WECC has identified videoconferences (initiated by the Entity) as "vendor remote access", which does not align with industry interpretation (NATF, other Regional Entities), so further clarification of this action would provide more clarity for future interpretations.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	

The ISO/RTO Council Standards Review Committee (IRC SRC) [1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems.

In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS.

That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term “authenticated” to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	

Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute’s response to Question 1.

Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

ISO/RTO Council Standards Review Committee (IRC SRC)[1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems.

In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS.

That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term “authenticated” to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	

Comment

Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	Yes
Document Name	

Comment

Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden

Likes 0	

Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Neil Shockey - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

See EEI's comments.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE agrees with restoring CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language, as well as addressing vendor remote access for EACMS and PACS in the newly formed Requirement R3.

However, Texas RE is concerned that in addressing vendor remote access for EACMS and PACS, the Standard Drafting Team (SDT) has elected to use the term “authenticated vendor-initiated remote connections.” Texas RE notes that “authenticated vendor-initiated remote connections” is not presently defined. As such, the introduction of such a term may create additional ambiguity, particularly around what constitutes an “authenticated” vendor-initiated remote connection. Texas RE suggests that the SDT could address this concern by using clarifying that such access includes “Interactive Remote Access and system-to-system remote access” as presently defined in the current and proposed Requirement 2.4 and 2.5.

Texas RE suggests the “hall of mirrors” concern could be better addressed by adding language to Requirement R3 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC appreciates the SDT's efforts to remove the "hall of mirrors" concerns, but suggests a return to the simpler approach for the requirements as discussed in its response to question #1. To support this reversion, GSOC recommends the following revision to the definition of EACMS to address the 'Hall of Mirrors" concern:Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. **This includes Intermediate Systems and does not include those systems that only perform electronic access control or electronic access monitoring to or from other EACMSs.**

GSOC suggests that incorporating the recommended revision above will address the "hall of mirrors" concern, which will allow the SDT to revert the proposed language to the simpler approach described in question 1 above and eliminate the need to create multiple requirements to address the same or similar security and access controls/objectives.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

We agree with the SDT on removing the hall of mirrors. But the "authentication" clarification below is necessary.

We request clarification of authenticating. The Technical Rationale, page 11 under R3, says this "authenticating" means authenticating the connection, not authenticating the user. This clarification should be in this Standard. This clarification is needed to avoid confusion with CIP-004.

We request clarification on the distinction between "connection" and "access."

Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State does not agree with the new terminology, as it is open to interpretation.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes the SDT should address this issue with requirements aimed at securing the management plane of EACMS rather than continuing down the path of perimeter-based security and bastion hosts (jump boxes and DMZs) as a sole protection for protected enclaves. This would clarify the recursive effect of “intermediate systems for intermediate systems ad nauseam.” This recursive effect problem seems related to the history of previous drafting teams endlessly debating whether a “packet to a port” is “access.” There may be a connection (a term with no recognized and easily specified meaning in NIST); however, a connection is generally not considered “authenticated” because “authentication” occurs at a different layer of the OSI model. Authentication is associated with sessions (ephemeral or time limited and specific to an interactive or programmed action) rather than connections (which are typically permanently configured, filtered, and existing at least in potential all the time, more associated with physical infrastructure as well).

There is a problem buried in current discussions of “authenticated” or ”provisioned” access that will continue to encourage entities to avoid more advanced technology such as next generation firewalls with role-based permissions. Currently, standard and extended access control lists based upon source, destination, and port/protocol contain no “authentication” mechanism. Filtering based upon source and destination is not a means of authentication. Therefore, a “packet to a port” to an EACMS that is allowed by source IP is a connection, and lacks authentication, but does not constitute “access.” Industry typically does not refer to “unauthenticated connections” but rather to authenticated or unauthenticated “sessions.” The SDT should conform to this more-common terminology because it tracks better with security principles and the technical implementations of authentication mechanism. Establishing a “session” to an EACMS to manage/configure it would constitute “access”, and require authentication and other security controls securing the management plane. Under this construct, requirements can be crafted to avoid the recursive perimeter protection problem.

Entities could design a solution where any unauthenticated connection, using only an IP source address to authorize passing the traffic, would avoid the requirement to detect active sessions entirely. This perverse incentive/loophole must be discouraged.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
While N&ST agrees that recursive requirements should be avoided, we believe the proposed changes do not address the possibility of an EACMS or PACS being located within an established Electronic Security Perimeter with sufficient clarity. N&ST recommends, in addition to moving R3 Parts 3.1 and 3.2 to R2 and eliminating R3, that "Applicability" language for those two Parts be modified to clarify that they apply to EACMS and PACS that are not located within any of the Responsible Entity's Electronic Security Perimeters.	
Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. The IRC SRC supports the removal of references to IRA and the undefined term “system to system” from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	

Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the removal of references to IRA and the undefined term "system to system" from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	

Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
It is important that the SDT clarify the applicable in-scope systems based on their risk to the Bulk Electric System and further clarify the role of Intermediate Systems and their capabilities and functions.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
MidAmerican supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modification and that it does help clarify the condition of elimination of a recursive requirement (hall of mirrors) and the Requirement is for the EACMS and PACS, and not the BCS,	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R3. However, ISO-NE recommends the use of consistent “vendor remote access” or “vendor-initiated remote connections” for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	

Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
These changes address the issues with undefined terms and broadens the scope appropriately.	
Likes 0	
Dislikes 0	

Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
If the SDT intends to exclude IRA requirements for EACMS or PACS, we suggest the SDT should clarify Intermediate Systems are not required for EACMS and PACS only if the EACMS and PACS are located outside ESP. We understand that the SDT didn’t use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without compliance with IRA requirements of CIP-005 R2?	
Likes 0	
Dislikes 0	

Response
Janet OBrien - WEC Energy Group, Inc. - 5
Answer	Yes
Document Name	
Comment
Agree with comments submitted separately by Tom Breene of WEC
Likes 0	
Dislikes 0	
Response
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy
Answer	Yes
Document Name	
Comment
Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2.
Likes 0	
Dislikes 0	
Response
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group
Answer	Yes
Document Name	
Comment
Likes 0	
Dislikes 0	
Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments on #1. Texas RE also suggests that defining "system-to-system" could add clarification.	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

See EEI's comments	
Likes 0	
Dislikes 0	
Response	

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC appreciates the SDT's proposal, but would offer that references to vendor-initiated remote access should be consistent throughout the body of the supply chain standards. In its review, GSOC identified the following different terms that appeared to be used either interchangeably or with the same or similar objectives:

- In CIP-005, GSOC identified the terms "active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)" in requirement R2.4; "active vendor remote access (including Interactive Remote Access and system-to-system remote access)" in requirement R2.5; and "authenticated vendor-initiated remote connections" in requirements R3.1 and 3.2.
- In CIP-013, GSOC identified the term "vendor-initiated remote access" in requirement R1.2.6.

All of these terms appear to have the same connotation and objective. Yet they are all slightly different in more ways than just reserving technical aspects for the more technical standards.

Utilization of different terms could lead to the interpretation of different scopes or objectives, which would result in confusion, ambiguity, and subjectivity in both implementation and compliance enforcement. Conversely, utilization of the same terms in multiple requirements makes the definition, scope, and objective clearer and simplier. It also makes implementation more straightforward and easier to audit.

For these reasons, GSOC suggests that the SDT consider defining vendor-initiated remote access and, then, utilize the defined term throughout the body of supply chain reliability standards to eliminate the potential for confusion regarding these undefined terms. To facilitate the SDT's review and potential adoption of this suggestion, GSOC proposes the following definition of vendor-initiated remote access:

User-initiated access by a Vendor employing a remote access client or other remote access technology using a routable protocol and is inclusive of Interactive Remote Access and system-to-system communications. Vendor is defined as those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services, but is not inclusive of other NERC registered entities providing reliability services.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA).	
Likes 0	
Dislikes 0	
Response	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
The phrase “coordinating controls” in Part 1.2.6 is not defined and should be clarified what it means explicitly.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	Yes
Document Name	

Comment

ISO-NE supports the removal of the references to IRA and the undefined term system-to-system for CIP-013-2. To avoid confusion, ISO-NE recommends that SDT ensures the CIP-013-2 R1.2.6 language and vendor terms remain consistent with the CIP-005 and CIP-010 supply chain requirements.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E believes this modification aligns CIP-013 Requirement P1.2.6 with the modifications made in CIP-005 and removes operational requirements from the CIP-013 plan.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
The SDT should ensure industry understands that CIP-013 Parts R1.2.5 and R1.2.6 are included as security controls required from the relationship of entities and vendors as part of an entities CIP-013 Supply Chain Cyber Security plan – i.e., when establishing a new supply chain vendor relationship with a vendor or enhancing the existing supply chain cyber security relationships. In general, the actions and outputs of a Supply Chain (and CIP-013) program occur before an entity onboards or maintains a system. The phrase “coordinating controls” is not defined nor well understood in CIP-013	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	

The IRC SRC supports the removal of references to IRA and the undefined term, “system to system” from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree that CIP-013 should remain the Plan while CIP-005 and CIP-010 are technical.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

The IRC SRC supports the removal of references to IRA and the undefined term, “system to system” from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	Yes
Document Name	

Comment

please reference Marty Hostler, Northern California Power Agency, comments

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes that the Standard Drafting Team (SDT) removed references to remote access and system-to-system communications from CIP-013-2 R1.2.6 and elected instead to define the term “remote access” in that proposed requirement as included “vendor-initiated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated [Interactive Remote Access (IRA)] and system to system access to BCS and PCAs” in the Technical Rationale document. Texas RE suggests that the SDT instead retain the general requirement that Requirement 1.2.6 apply to system-to-system remote access directly within the requirement language. Texas RE further suggests that the SDT could address concerns regarding the requirement that EACMS and PACS themselves have intermediate systems by adding language to Requirement R1.2.6 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point, obviating the need for the proposed changes to CIP-013-2 R1.2.6.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Unfortunately, there is a continual misplacement and shift of requirements (Parts) related to their given security objectives within the CIP framework. NERC is chartered with the edict to map CIP to NIST and the SDT should keep this in mind when developing standards.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E cannot agree the modifications are cost effective since the work to complete the implementation of the CIP-013-1 set of Standards is just being completed and full testing has not been completed to determine the cost of that work. As noted in the PG&E input on the first Comment & Ballot for these modifications, PG&E would have preferred to have an “Unknown” option to select.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Do not agree. Tri-State contends that the edits should have been risk-based and only applicable to the control portions of PACS and EACMS, and not also the monitoring portions of those systems.

Additionally, time and resources would be saved if the SDT would include language that clarifies that entity-initiated remote access and entity-initiated vendor remote access are not prohibited by CIP standards.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Although ISO-NE acknowledges the importance of establishing Supply Chain requirements associated with EACMS and PACS, ISO-NE respectfully believes that it cannot clearly determine if the modified requirements would meet the FERC directives in a cost effective manner because the current CIP-005-6, CIP-010-3 and CIP-013-1 standards have yet to become effective. It is difficult to determine cost-effectiveness when the approach is to build on requirements that the Industry has had limited experience with and limited opportunities for lessons learned or to mature processes and controls.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

“vendor-initiate remote access” only seems to apply to R3 of CIP-005-7, so the summary above does not accurately reflect the changes to R2 of CIP-005-7. “Vendor Initiated” should be included in CIP-007 R2.4 and 2.5. Leaving non-vendor initiated remote access in R2.4 and R2.5 is purely administrative in nature. SMUD has implemented this requirement as it is currently written and have found it to be both operationally inefficient and lacking value from a security standpoint.

For R3, this question cannot be answered because it is unclear what constitutes an authenticated vendor-initiated remote connection.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
To minimize churn among standard versions and better identify the scope, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-005-7, CIP-010-4, and CIP-013-2 with other existing drafting teams for related standards; specifically, Projects 2016-02, 2020-03, and 2020-04. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends changing the applicability around PACS to be associated with Medium Impact BCS with ERC instead of just Medium Impact BCS to avoid confusion. The modifications under CIP-010-4 R1.6 to include PACS associated with Medium Impact BES Cyber Systems is otherwise out of alignment in regards to the application of PACS under the CIP standards. The CIP standards under CIP-006-6 require the application of PACS in environments associated with High Impact BES Cyber Systems, Medium Impact BES Cyber Systems with External Routable Connectivity, and associated EACMS and PCAs but do not require this for Medium Impact BES Cyber Systems *without* ERC. By expanding the requirement and application of PACS to Medium Impact BES Cyber Systems without any qualifier per CIP-010-4 R1.6, it is not clear whether this is implied to bring into scope similar or identical cyber assets to PACS that may be used by entities to restrict and/or monitor access to Medium Impact without ERC BES Cyber Systems but which would not meet the definition of PACS (even though the application of these are not required by the standards).	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The basic capability of detecting (which is a better term than determine) remote session activity is the relevant security control. Whether that activity is initiated by a vendor, partner, customer, or an employee is irrelevant to the technical capability. Scoping the requirement narrowly does not provide significant cost savings and still allows for poor security. BPA does not agree with feedback that monitoring for remote sessions by employees could be a union issue. There is a difference between monitoring for external sessions vs monitoring employee activity within a session and this requirement does not go that far. Insider threat remains the number one threat to critical infrastructure and the ability to actively detect and terminate a session regardless of who originates it is a key cyber security control.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST recommends modifying proposed changes to CIP-005, as per our response to Question 1.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	Yes
Document Name	

Comment

please reference Marty Hostler, Northern California Power Agency, comments

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment
GSOC agrees that the SDT has worked to fine tune requirements to ensure security and cost-effectiveness. However, GSOC remains concerned about the scope of EACMSs to which the requirements are applicable and how the current scope increases the overall cost and burden on registered entities. For these reasons, GSOC recommends that the SDT work on additional fine-tuning of the overall scope of applicability as related to EACMSs. Additionally, GSOC notes that the multiple requirements, “interchangeable” terms, and potential for confusion and ambiguity detract from the potential cost-effectiveness of these standards. The elimination of multiple, “interchangeable” terms through the use of definitions and defined terms along with streamlined requirements will help to further fine-tune the scope and security obligations set forth within these standards. They will also facilitate consistent, effective compliance auditing, making these reliability standards more cost-effective across the ERO Enterprise.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	

Comment
Cost effective is vague. Please provide a cost/benefit justification for any posposed changes.

Likes 0	
Dislikes 0	

Response

Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	

Comment
Agree with comments submitted separately by Tom Breene of WEC

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We recommend defining the term ‘Vendor Initiated Remote Access’, and define who is considered a vendor.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	

Document Name	
Comment	

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits.

In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment
Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks

Answer	
Document Name	

Comment
While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits. In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	
Document Name	

Comment

No comment on cost effectiveness of the proposed changes.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Neil Shockey - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

See EEI's comments

Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools.	
Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments for the standard drafting team to consider, if desired.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	
The wording in CIP-013 R1.2.6 should match the wording in CIP-005-7 R3 P3.2, to wit: “authenticated vendor-initiated remote connections”	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
The SDT uses the term “sessions” in CIP-005-7 R2 but in CIP-005-7 R3, it proposes replacing the term “session” with “connection.” Since there is no definition of “connection” in the *Glossary of Terms Used in NERC Reliability Standards* or in the NIST online glossary, BPA believes the term “connection” is ambiguous and should not be used within the standard. Proposed change to CIP-005-7 R3.1: Have one or more method(s) for detecting remote access sessions. Proposed change to CIP-005-7 R3.2: Have one or more method(s) for terminating remote access sessions.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	
Document Name	
Comment	
Further clarity should be provided regarding the definition of “vendor” in relation to staff augmentation consultants/contractors who may performing system integration work or supporting/managing the operation of BES Cyber Assets via remote access. NERC had during CIP-013-1 standard development responses to industry, indicated that it does not consider staff augmentation contractors/consultants who are treated similar to employees	

to be considered vendors. However, WECC is communicating a different approach in compliance outreach sessions and are expecting entities to identify staff augmentation contractors/consultants to be considered as vendors due to risks they could pose. This should be clarified within the standards to either allow entities the flexibility to define who vendors are to them ***or*** to have the standard drafting team define this clearly through a proposed Glossary defined term or within the standard language itself as the current definition within the standard is open to interpretation between enforcement entities and create undue compliance burden.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment

In regards to CIP-010-4 Requirement 1 Part 1.6, PCAs should also be included in the Applicable Systems. When BES Cyber Systems and PCAs are located within the same ESP and software is validated and verified for the BCS but not the PCAs, a mixed-trust security environment is created within an ESP. By not including PACs in the Applicable Systems, it poses additional unnecessary risk to the security of the BES.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	
Document Name	

Comment

The language is very clear in this version.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	
Document Name	

Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E has no additional input regarding this Comment & Ballot.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
MEC supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

See EEI's comments

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

Regarding the Implementation Guidance for CIP-005-7, we provide the following four (4) comments:

(1) Page 3, 2nd paragraph - Suggest adding 'within the Electronic Security Perimeter' as EACMS can reside within the ESP and this appears to be the context of these EACMS.

(2) 'However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS,'

Change to "However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS within the Electronic Security Perimeter,[…]"

(3) Page 5, 2b 'Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture'

Suggest different wording than architecture. Perhaps network topology?

(4) Page 7 - While this section contains a “cut and paste” of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is from the CIP-005-6 standard, consider detailing the first use of EAP as it isn't used anywhere prior in the IG. Change 'Responsible Entities should know what traffic needs to cross an EAP' to "Responsible Entities should know what traffic needs to cross an Electronic Access Point (EAP)..."

Likes 0	
Dislikes 0	

Response

Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	
The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	

We appreciate the SDT efforts.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	
Document Name	

Comment

Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute's response to Question 5.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	

Comment

In the Technical Rationale for Reliability Standard CIP-013-2 document (page 11), "Requirement R2" should read "Requirement R3". The text indicates "The proposed requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk

management controls (P.46) ". R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Comments from EEI

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for

EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

☒ Yes

☐ No

Comments: While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we recommend the SDT revise "vendor remote access" to "vendor initiated remote access" or explain why all vendor remote access needs to be evaluated for Parts 2.4 and 2.5.

EEI supports the current proposed draft language for Requirement R3.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments: EEI supports the changes made by the SDT to address prior EEI member comments related to the "hall of mirrors" issue.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments:

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments: EEI has no comment on the cost effectiveness of the proposed changes.

5. Provide any additional comments for the standard drafting team to consider, if desired.

Comments: EEI previously provided comments that CIP-005-7 did not provide sufficient clarity regarding contractors who are essential to the reliable operation of the BES. Specifically, the Reliability Standard did not provide a mechanism that exempted contractors who provided essential contract services. Although CIP-005-7 does not explicitly provide a defined process for exempting these contractors, the draft Implementation guidance makes it clear that these types of contractors are to be handled in a manner similar to the staff of a registered entity.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2019-03 Cyber Security Supply Chain Risks | CIP-005-7, CIP-010-4, & CIP-013-2 (Draft 3)
Comment Period Start Date:	7/28/2020
Comment Period End Date:	9/10/2020
Associated Ballot:	2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 3 ST

There were 59 sets of responses, including comments from approximately 135 different people from approximately 85 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISONE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Ali Miremadi	CAISO	2	WECC
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
CMS Energy - Consumers Energy Company	Jeanne Kurzynowski	3,4,5	RF	Consumers Energy Company	Jeanne Kurzynowski	Consumers Energy Company	1,3,4,5	RF
					Jim Anderson	Consumers Energy Company	1	RF
					Karl Blaszkowski	Consumers Energy Company	3	RF
					Theresa Martinez	Consumers Energy Company	4	RF
					David Greyerbiehl	Consumers Energy Company	5	RF
ACES Power Marketing	Jodirah Green	1,3,4,5,6		ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC			Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Mark Garza	FirstEnergy - FirstEnergy Corporation	4	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Randy MacDonald	NB Power Corporation	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment

N&ST believes there are several problems with proposed requirement R3 as presently written

- It addresses "authenticated vendor-initiated remote connections" without explicitly establishing a requirement for authentication, nor does it provide a working definition of a "remote connection."
- Part 3.2's mandate to control the ability of a vendor whose connection has been terminated to reconnect creates a consistency problem. There is no comparable requirement in Requirement R2 for vendor remote connections to BES Cyber Systems and PCAs.
- A second inconsistency is created by using the term, "remote connection" in R3, whereas the term, "remote access" is used in R2.

N&ST recommends the following changes:

- Move R3's proposed Parts 3.1 and 3.2 to R2 and eliminate R3. N&ST sees no need to address vendor remote access to applicable systems in two separate, top-level requirements.
- Modify the "applicability" language in those two Parts to say, for example:
    - "EACMS and PACS:
    - associated with High Impact BES Cyber Systems, and
    - not located within any of the Responsible Entity's Electronic Security Perimeter(s)."
        - NOTE: 2nd bullet is taken verbatim from the Glossary definition of IRA
- Add an explicit requirement to use at least one form of authentication.

• Consider adding language, taken from the existing IRA definition, that that clarifies "vendor remote access" originates from "Cyber Assets used or owned by vendors, contractors, or consultants." The SDT may want to consider adding this to existing R2 Parts 2.4 and 2.5, as well. • Change “remote connection” to “remote access” • The proposed requirement to control vendor reconnection should either be eliminated or added to existing R2 Part 2.5.	
Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	
Response Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report. Industry was also concerned about ambiguity in the phrase ‘vendor remote access’, and how it could lead to varied interpretations that an attempt to establish a session ‘***to***’ an EACMS that is later denied ‘***by***’ the EACMS could be considered ‘access’. A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

ACES does not agree with the use of “authenticated” and “remote connections” in R3.

R3 without the word authenticated, covers all vendor connections .. CIP-004 R4.1 already requires access management for EACMS and PACS and CIP-007 R5.1 requires methods to enforce authentication. Further, as discussed on the project 2019-03 webinar, unauthenticated remote access is already addressed by the CIP standards. Lastly, an authorized remote connection can be made without being authenticated. Thus an authorized malicious insider could easily craft a denial of service without ever being completely authenticated. Removing the word “authenticated” would put more emphasis on **all** vendor connections and increases the security objective of R3. Suggested language:

“Have one or more method(s) to determine vendor initiated remote access.”

Secondly, the CIP standards have always used the NERC defined term: Interactive Remote Access and or remote access vs what is in the draft “remote connections”. ACES suggests using language consistent with existing standards. Without defining “remote connections”, it makes the requirement vague and could be interpreted differently. Suggested language:

“Have one or more method(s) to terminate vendor initiated remote access and control the ability to reconnect.”

Likes 0	
Dislikes 0	

Response: Thank you for your response. The SDT agrees with this perspective on CIP-004 and CIP-007; however, the changes that were made were specific to external vendor-initiated remote access.

The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA proposes the SDT eliminate references to “vendor.” The requirements should apply to any active remote sessions.

Proposed change to R2.4:

Have one or more methods for determining detecting active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Proposed change to R2.5:

Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response:
Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the “Hall of mirrors”) that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added

EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report. Industry was also concerned about ambiguity in the phrase 'vendor remote access', and how it could lead to varied interpretations that an attempt to establish a session '***to***' an EACMS that is later denied '***by***' the EACMS could be considered 'access'. A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment
Restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language is fine, but the language in R3 is unclear. It's not clear what "authenticated vendor-initiated" remote connections are. The intent seems clear, and the security necessity is warranted, but it is not clear why using something like "Have one or more method(s) for determining authorized vendor-initiated remote access connections" is not used. What value does using "authenticated" vendor-initiated remote access connections add? Why is "Remote Connections" used instead of "Remote Access" since R3 is "Vendor Remote Access"? What is considered a remote connection? Does a remote connection include both system to system communication and remote access? Is a remote connection from outside of an entities corporate network or is it a remote connection from inside an entities network but behind a firewall and using some remote access client?

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below: • A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

- "Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to 'how' authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

The SDT determined to not define the term "Remote" because it is context dependent (i.e., external to your corporate network versus external to your ESP, etc.).

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
If the requirements are technically the same, as it appears, then the new scope should be added to Parts 2.4 and 2.5. However, we believe the SDT was attempting to resolve some ambiguity that currently exists around what is vendor remote access. We commend the SDT for this effort, and request they clarify the existing requirements (parts 2.4 and 2.5). Specifically, vendor remote access should be defined or somehow clarified that it only includes access where the vendor's personnel or system has direct access and ability to control the session. Having IRA and system-to-system listed as examples, but not an all-inclusive list, would also be helpful.	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the "Hall of mirrors") that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently

approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report. Industry was also concerned about ambiguity in the phrase 'vendor remote access', and how it could lead to varied interpretations that an attempt to establish a session '***to***' an EACMS that is later denied '***by***' the EACMS could be considered 'access'. A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

The SDT should provide guidance or clarify the role or function of Intermediate Systems in context of providing electronic access to EACMS and PACS located within an ESP vs outside an ESP.

If the SDT intends to *exclude* Interactive Remote Access (IRA) requirements for EACMS or PACS in CIP-005-7 R3.1 and R3.2, it should clarify that an intermediate system is not required to electronically access an EACMS and PACS located outside an ESP. However, if the EACMS or PACS is located within the ESP, the entity is required to utilize an Intermediate System for electronic access. This brings into scope all CIP-005 R2 requirements.

Without guidance, entities may interpret that an Intermediate System is never required for the vendor IRA to EACMS or PACS - even though they may exist within an ESP.

The SDT did not use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without the IRA requirements of CIP-005 R2?

The SDT could consider putting all vendor remote access sub-requirements in one requirement – 3.0.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
Agree with leaving R2 as is. Disagree with need for a R3. Actually, the SDT should be providing us with a cost/benefit justification for change.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. During the second ballot, the SDT realized how problematic this was after industry expressed concern about Parts 2.4 and 2.5 moving into R3, and effectively creating a recursive requirement (also known as the "Hall of mirrors") that would have required use of Intermediate System for vendor-initiated remote access to an EACMS. Since an Intermediate System is an EACMS by definition, this unintended consequence could have created a potential never-ending condition and an impossibility to comply, so we took that very seriously. The SDT listened to these concerns, and resolved this by restoring Parts 2.4 and 2.5 to the original currently	

approved CIP-005-6 language and Applicable Systems, and we not proposing any modifications to those two parts. Instead, the SDT refocused on the FERC Order and the SAR scope and is proposing R3 be dedicated specifically to EACMS and PACS associated to high and medium impact BES Cyber Systems. Here you see the redline for the newly proposed parent Requirement R3, where the SDT: Added EACMS address the directive in FERC Order 850, and Added PACS to address the recommendation in the NERC Cyber Security Supply Chain Risks Report. Industry was also concerned about ambiguity in the phrase 'vendor remote access', and how it could lead to varied interpretations that an attempt to establish a session '***to***' an EACMS that is later denied '***by***' the EACMS could be considered 'access'. A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
We thought a CIP Modification SDT goal was to remove this language to assist the coming virtualization updates. Request clarification on why CIP-005 R2 Parts 2.4 & 2.5 use the phrase "vendor remote access" while CIP-013 R1 Part 1.2.6 uses the phrase "vendor-initiated remote access" We are concerned that omitting "initiated" may introduce unintended requirements in CIP-005.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Project 2019-03 had a FERC directive to meet and the 2016-02 team will make conforming changes to the approved CIP-005-7 to enable virtualization going forward while maintaining backwards compatibility.	

In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC greatly appreciates the drafting team's efforts and thoughtful approach regarding this proposal. However, it is concerned that the splitting of these requirements creates significant potential for very different compliance obligations for the different classes of assets while attaining the same or similar cyber security protections as would be garnered solely with either set of requirements. More specifically, the differentiation between the requirements for PACS and EACMSs and the assets to which access is sought is likely to cause confusion as well as increase the potential for differing interpretations of compliance and "double jeopardy." That the proposed split of requirements would likely provide little or no additional security benefit, while being unduly burdensome for entities, creates additional concerns for responsible entities as they try to focus their resources on those activities that will have a net effect of enhancing security. GSOC understands that industry comments have driven these proposed changes, and agrees that valid concerns have been presented (e.g., the hall of mirrors). In its response to question #2, GSOC proposes an approach to addressing these previous concerns and comments that will allow a return to a simpler approach for the requirements generally. We respectfully recommend that the SDT consider utilizing alternative approaches such as are proposed below, e.g., definition revision, to allow the requirements to more clearly and succinctly meet the Commission directives regarding EACMS and PACS. This simpler approach to address concerns will facilitate a reversion of the requirement language to the initial proposal where EACMSs and PACs were added as applicable systems for the existing requirements.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT considered the proposed revisions suggested in question 2 and determined that the proposed definition recreates the hall of mirrors issue. The SDT asserts that requirement R2 and R3 are mutually exclusive requirements with mutually exclusive systems and does not create double jeopardy.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to Marty Hostler.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with restoring R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and adding R3 for EACMS and PACS.	
Likes 0	
Dislikes 0	

Response Thank you for your comment.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We recommend that view only access by a vendor is not considered IRA, nor vendor remote access.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. This comment has been turned over to NERC compliance for review.	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
To separate the remote access from the vendor remote access, FirstEnergy would respectfully suggest that the currently drafted R2 Parts 2.4 and 2.5 are reorganized to become R3 Parts 3.1 and 3.2. Subsequently, the currently drafted R3 3.1 and 3.2 become Parts 3.3 and 3.4.	
Likes 0	
Dislikes 0	

Response Thank you for your comment. The changes you are requesting were contained in draft 2 of the standards and was voted down by industry due to the recursive nature of the requirements that it introduced. This new requirement R3 is mutually exclusive from R2 and its parts.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to WECC.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to EEI's comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R2 Parts 2.4 and 2.5. However, ISO-NE recommends the use of consistent "vendor remote access" or "vendor-initiated remote connections" for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E believes this is the appropriate modifications in-line with the industry comments made to the second Comment & Ballot. The restoration of the P2.4 and P2.5, along with the modifications made in Requirement R3 more clearly eliminate the potential interpretation that could have resulted in recursive requirements noted in Question 2 below.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
MidAmerican supports EEI commnets	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to EEI.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to EEI.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy supports EEI's comments on Q1:

"While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we ask the SDT to consider revising “vendor remote access” to “vendor initiated remote access” or provide clarification why they believe that all vendor remote access should be considered under Parts 2.4 and 2.5.

EEI supports the current proposed draft language for Requirement R3."

In addition, NVE supports the revision of "vendor remote access" to "vendor initiated remote access" due to current conflicting interpretations of P2.5 and 2.5 and CIP-005-6 by Regional Entities. WECC has identified videoconferences (initiated by the Entity) as "vendor remote access", which does not align with industry interpretation (NATF, other Regional Entities), so further clarification of this action would provide more clarity for future interpretations.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC’s Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC’s Compliance & Enforcement team, who can assess and unify audit interpretation.

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The ISO/RTO Council Standards Review Committee (IRC SRC) [1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems. In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS. That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term “authenticated” to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020. [1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT recommends reviewing the Technical Rationale, which states the below: • A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating. • "Authentication" is the mechanism for the EACMS or PACS to identify the user or device. • This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to 'how' authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	Yes
Document Name	

Comment
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute's response to Question 1.

Likes 0	
Dislikes 0	

Response Thank you for your comments, please see response to EEI.
Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

ISO/RTO Council Standards Review Committee (IRC SRC)[1] supports the restoration of CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original, currently approved CIP-005-6 language and Applicable Systems.

In addition, we agree with the addition of Requirement R3, Parts 3.1 and 3.2 to focus on the directive in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report to have one or more methods to determine and be able to terminate vendor-initiated remote connections to EACMS and PACS.

That said, the IRC SRC requests the Standard Drafting Team (SDT) provide additional clarity around the term "authenticated" to align and memorialize what was verbally (and non-binding) presented by the SDT in the Project 2019-03 webinar (timestamp 9:00 – 10:00 of 37:24) on August 5, 2020.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- "Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to 'how' authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes

Document Name	
Comment	
Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT understand the subtle differences in the language and because of the differences in the assets in the applicability section, the SDT concluded that the differences in language were required so as to not introduce unintended consequences i.e. hall of mirrors effect. The SDT has documented rationale in the Technical Rationale document associated with CIP-005-7.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Requirements R2 and R3 have subtly different language (e.g. "disable" vs. "terminate" and "vendor-initiated") in addition to different applicability. Matching the language or updating the language so the same processes developed for R2 could be used for R3 would reduce regulatory burden	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understand the subtle differences in the language and because of the differences in the assets in the applicability section, the SDT concluded that the differences in language were required so as to not introduce unintended consequences i.e. hall of mirrors effect. The SDT has documented rationale in the Technical Rationale document associated with CIP-005-7.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE agrees with restoring CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language, as well as addressing vendor remote access for EACMS and PACS in the newly formed Requirement R3.

However, Texas RE is concerned that in addressing vendor remote access for EACMS and PACS, the Standard Drafting Team (SDT) has elected to use the term “authenticated vendor-initiated remote connections.” Texas RE notes that “authenticated vendor-initiated remote connections” is not presently defined. As such, the introduction of such a term may create additional ambiguity, particularly around what constitutes an “authenticated” vendor-initiated remote connection. Texas RE suggests that the SDT could address this concern by using clarifying that such access includes “Interactive Remote Access and system-to-system remote access” as presently defined in the current and proposed Requirement 2.4 and 2.5.

Texas RE suggests the “hall of mirrors” concern could be better addressed by adding language to Requirement R3 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see response to EEI.

Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC appreciates the SDT's efforts to remove the "hall of mirrors" concerns, but suggests a return to the simpler approach for the requirements as discussed in its response to question #1. To support this reversion, GSOC recommends the following revision to the definition of EACMS to address the 'Hall of Mirrors" concern:Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. **This includes Intermediate Systems and does not include those systems that only perform electronic access control or electronic access monitoring to or from other EACMSs.** GSOC suggests that incorporating the recommended revision above will address the "hall of mirrors" concern, which will allow the SDT to revert the proposed language to the simpler approach described in question 1 above and eliminate the need to create multiple requirements to address the same or similar security and access controls/objectives.	
Likes 0	
Dislikes 0	
Response Thank you for your comments. At this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT believes that the suggested definition would recreate the hall of mirrors issue which was addressed by creating R3.1 and R3.2.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
We agree with the SDT on removing the hall of mirrors. But the “authentication” clarification below is necessary. We request clarification of authenticating. The Technical Rationale, page 11 under R3, says this “authenticating” means authenticating the connection, not authenticating the user. This clarification should be in this Standard. This clarification is needed to avoid confusion with CIP-004. We request clarification on the distinction between “connection” and “access.”	
Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

CIP-005-7 Requirement R3 picks up after the user or device has already used its authorized vendor remote access to make an authenticated connection. The CIP-005-7 Requirement R3 controls focus on the connection itself and not the access.

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	
Comment	
Tri-State does not agree with the new terminology, as it is open to interpretation.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response Thank you for your comment. The SDT has prepared implementation guidance and technical rationale to assist industry.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the SDT should address this issue with requirements aimed at securing the management plane of EACMS rather than continuing down the path of perimeter-based security and bastion hosts (jump boxes and DMZs) as a sole protection for protected enclaves. This would clarify the recursive effect of “intermediate systems for intermediate systems ad nauseam.” This recursive effect problem seems related to the history of previous drafting teams endlessly debating whether a “packet to a port” is “access.” There may be a connection (a term with no recognized and easily specified meaning in NIST); however, a connection is generally not considered “authenticated” because “authentication” occurs at a different layer of the OSI model. Authentication is associated with sessions (ephemeral or time limited and specific to an interactive or programmed action) rather than connections (which are typically permanently configured, filtered, and existing at least in potential all the time, more associated with physical infrastructure as well). There is a problem buried in current discussions of “authenticated” or ”provisioned” access that will continue to encourage entities to avoid more advanced technology such as next generation firewalls with role-based permissions. Currently, standard and extended access control lists based upon source, destination, and port/protocol contain no “authentication” mechanism. Filtering based upon source and	

destination is not a means of authentication. Therefore, a “packet to a port” to an EACMS that is allowed by source IP is a connection, and lacks authentication, but does not constitute “access.” Industry typically does not refer to “unauthenticated connections” but rather to authenticated or unauthenticated “sessions.” The SDT should conform to this more-common terminology because it tracks better with security principles and the technical implementations of authentication mechanism. Establishing a “session” to an EACMS to manage/configure it would constitute “access”, and require authentication and other security controls securing the management plane. Under this construct, requirements can be crafted to avoid the recursive perimeter protection problem. Entities could design a solution where any unauthenticated connection, using only an IP source address to authorize passing the traffic, would avoid the requirement to detect active sessions entirely. This perverse incentive/loophole must be discouraged.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The Project 2016-02 SDT will make conforming changes once Project 2019-03 completes. CIP-005-7 Requirement R3 picks up after the user or device has already used its authorized vendor remote access to make an authenticated connection. The CIP-005-7 Requirement R3 controls focus on the connection itself and not the access.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
While N&ST agrees that recursive requirements should be avoided, we believe the proposed changes do not address the possibility of an EACMS or PACS being located within an established Electronic Security Perimeter with sufficient clarity. N&ST recommends, in addition to moving R3 Parts 3.1 and 3.2 to R2 and eliminating R3, that "Applicability" language for those two Parts be modified to clarify that they apply to EACMS and PACS that are not located within any of the Responsible Entity's Electronic Security Perimeters.	
Likes 0	

Dislikes 0	

Response
Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	Yes
Document Name	

Comment

please reference Marty Hostler, Northern California Power Agency, comments

Likes 0	
Dislikes 0	

Response
Thank you for your comment, please see response to Northern California Power Agency.

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

The CAISO supports the ISO/RTO Council Standards Review Committee comments below.

The IRC SRC supports the removal of references to IRA and the undefined term “system to system” from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute’s response to Question 2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the removal of references to IRA and the undefined term “system to system” from CIP-005-7, requirement R3, Parts 3.1 and 3.2 to clarify that Intermediate Systems are optional and not required for EACMS or PACS.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

It is important that the SDT clarify the applicable in-scope systems based on their risk to the Bulk Electric System and further clarify the role of Intermediate Systems and their capabilities and functions.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In the last posting the SDT believes that the requirements are clarified based on risk by reverting back to Requirement R2.4 and R2.5 and adding Requirement R3 for EACMS and PACS.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
MidAmerican supports EEI comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the modification and that it does help clarify the condition of elimination of a recursive requirement (hall of mirrors) and the Requirement is for the EACMS and PACS, and not the BCS,	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE agrees with the proposed approach to restore the CIP-005-7 Requirements R3. However, ISO-NE recommends the use of consistent “vendor remote access” or “vendor-initiated remote connections” for both Requirement R2 Part 2.4 and R2.5 and the Requirement R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes

Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
These changes address the issues with undefined terms and broadens the scope appropriately.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

If the SDT intends to exclude IRA requirements for EACMS or PACS, we suggest the SDT should clarify Intermediate Systems are not required for EACMS and PACS only if the EACMS and PACS are located outside ESP. We understand that the SDT didn't use the defined term IRA in R3.1 and R3.2, but if an EACMS or PACS is inside an ESP and the vendor remote access meets the IRA definition, does SDT allow a vendor IRA to the EACMS or PACS inside an ESP without compliance with IRA requirements of CIP-005 R2?	
Likes 0	
Dislikes 0	
Response Thank you for your comment. It is not within the scope of the 2019-03 SAR for the SDT to resolve regional interpretation inconsistencies regarding dual classification of EACMS and/or PACS installed inside an ESP and the varied implications on Intermediate System need. The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC's Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC's Compliance & Enforcement team, who can assess and unify audit interpretation.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to WECC.	

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments on #1. Texas RE also suggests that defining "system-to-system" could add clarification.	
Likes 0	
Dislikes 0	
Response Thank you for your comment, please see response to question 1. "System-to-system" is already part of the approved language of the standard and this drafting team did not make modifications to that terminology.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC appreciates the SDT's proposal, but would offer that references to vendor-initiated remote access should be consistent throughout the body of the supply chain standards. In its review, GSOC identified the following different terms that appeared to be used either interchangeably or with the same or similar objectives:

- In CIP-005, GSOC identified the terms "active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)" in requirement R2.4; "active vendor remote access (including Interactive Remote Access and system-to-system remote access)" in requirement R2.5; and "authenticated vendor-initiated remote connections" in requirements R3.1 and 3.2.
- In CIP-013, GSOC identified the term "vendor-initiated remote access" in requirement R1.2.6.

All of these terms appear to have the same connotation and objective. Yet they are all slightly different in more ways than just reserving technical aspects for the more technical standards.

Utilization of different terms could lead to the interpretation of different scopes or objectives, which would result in confusion, ambiguity, and subjectivity in both implementation and compliance enforcement. Conversely, utilization of the same terms in multiple requirements makes the definition, scope, and objective clearer and simplier. It also makes implementation more straightforward and easier to audit.

For these reasons, GSOC suggests that the SDT consider defining vendor-initiated remote access and, then, utilize the defined term throughout the body of supply chain reliability standards to eliminate the potential for confusion regarding these undefined terms. To

facilitate the SDT's review and potential adoption of this suggestion, GSOC proposes the following definition of vendor-initiated remote access: User-initiated access by a Vendor employing a remote access client or other remote access technology using a routable protocol and is inclusive of Interactive Remote Access and system-to-system communications. Vendor is defined as those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services, but is not inclusive of other NERC registered entities providing reliability services.	
Likes 0	
Dislikes 0	
Response Thank you for your comments. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for "authenticated vendor-initiated remote connections." However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase "vendor-initiated remote access" included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope. Vendor is not a defined term, however as written by the original Project 2016-03 SDT and included in the CIP-013-2 Technical Rationale "A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the removal of the references to Interactive Remote Access (IRA).	
Likes 0	
Dislikes 0	
Response	

Response Thank you for your comment.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to WECC.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
The phrase “coordinating controls” in Part 1.2.6 is not defined and should be clarified what it means explicitly.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. When considering a vendor, part of the entity process should be to gain an understanding of how the vendor communicates breaches or vulnerabilities, and then determine what risk the vendor's approach poses. Entities might have established their own standards and expectations for how quickly they expect to be notified of such things and as a part their plan may incorporate certain expectations or legal obligations into the procurement terms with the vendor. These controls in CIP-013 are intended to provide a minimum set of upfront considerations the entity should consider when assessing risk prior to procurement. The operationalization of these controls occurs after the CIP-013 planning requirements are already met. As written by the original Project 2016-03 drafting team, each entity has the flexibility to develop their own risk-based plan to address vendor risk.	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	

ISO-NE supports the removal of the references to IRA and the undefined term system-to-system for CIP-013-2. To avoid confusion, ISO-NE recommends that SDT ensures the CIP-013-2 R1.2.6 language and vendor terms remain consistent with the CIP-005 and CIP-010 supply chain requirements.	
Likes 0	
Dislikes 0	
Response Thank you for your comments. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for "authenticated vendor-initiated remote connections." However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase "vendor-initiated remote access" included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes this modification aligns CIP-013 Requirement P1.2.6 with the modifications made in CIP-005 and removes operational requirements from the CIP-013 plan.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
The SDT should ensure industry understands that CIP-013 Parts R1.2.5 and R1.2.6 are included as security controls required from the relationship of entities and vendors as part of an entities CIP-013 Supply Chain Cyber Security plan – i.e., when establishing a new supply chain vendor relationship with a vendor or enhancing the existing supply chain cyber security relationships. In general, the actions and outputs of a Supply Chain (and CIP-013) program occur before an entity onboards or maintains a system. The phrase “coordinating controls” is not defined nor well understood in CIP-013	
Likes 0	
Dislikes 0	
Response Thank you for your comments. These CIP-013 requirements are not operational requirements. Those are items to have in your procurement plan and things to consider when doing business with vendors, and then they have “like” parts in the operational standards where day to day execution occurs. These are complimentary requirements with complimentary objectives, and not duplicative nor competing activities with CIP-005-7 R2-R3 and CIP-010-3 R1.6. When considering a vendor, part of the entity process should be to gain an understanding of how the vendor communicates breaches or vulnerabilities, and then determine what risk the vendor’s approach poses. Entities might have established their own standards and expectations for how quickly they expect to be notified of such things and as a part their plan may incorporate certain expectations or legal obligations into the procurement terms with the vendor. These controls in CIP-013 are intended to provide a minimum set of upfront considerations the entity should consider when assessing risk prior to procurement. The operationalization of these controls occurs after the CIP-013 planning requirements are already met. As written by the original Project 2016-03 drafting team, each entity has the flexibility to develop their own risk-based plan to address vendor risk.	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the removal of references to IRA and the undefined term, “system to system” from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree that CIP-013 should remain the Plan while CIP-005 and CIP-010 are technical.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. The IRC SRC supports the removal of references to IRA and the undefined term, “system to system” from CIP-013-2, requirement R1.2.6. In addition, we agree with the addition of EACMS and PACS to meet what was directed in FERC Order 850 and the recommendation in the NERC Cyber Security Supply Chain Risks Report.	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments.	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response The SDT thanks you for your comments. Please see response to Northern California Power Agency.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes that the Standard Drafting Team (SDT) removed references to remote access and system-to-system communications from CIP-013-2 R1.2.6 and elected instead to define the term “remote access” in that proposed requirement as included “vendor-initiated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated [Interactive Remote Access (IRA)] and system to system access to BCS and PCAs” in the Technical Rationale document. Texas RE suggests that the SDT instead retain the general requirement that Requirement 1.2.6 apply to system-to-system remote access directly within the requirement	

language. Texas RE further suggests that the SDT could address concerns regarding the requirement that EACMS and PACS themselves have intermediate systems by adding language to Requirement R1.2.6 that excludes Intermediate Systems for EACMS and PACS in the applicability section. Alternatively, the SDT could revise the definition of Interactive Remote Access to clarify this point, obviating the need for the proposed changes to CIP-013-2 R1.2.6.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for "authenticated vendor-initiated remote connections." However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase "vendor-initiated remote access" included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope. The SDT decided not to change definition of IRA or any NERC defined terms since that change would impact other existing Standards and that is beyond the scope of this SDT's SAR. In addition, Project 2016-02 is currently reviewing this definition and this comment will be passed to that team for consideration.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

SDT Response Below:

Thank you for your comments. The SDT understand there are cost considerations with every change to a standard. The Project 2019-03 SDT modified the Supply Chain Standards as detailed in the SAR and the team believes that the changes balance added security with the directives from FERC Order 850 and the recommendations in the NERC Supply Chain Report.

Barry Jones - Barry Jones On Behalf of: Erin Green, Western Area Power Administration, 1, 6; sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Unfortunately, there is a continual misplacement and shift of requirements (Parts) related to their given security objectives within the CIP framework. NERC is chartered with the edict to map CIP to NIST and the SDT should keep this in mind when developing standards.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see the response at the beginning of question 4.

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	
Comment	
PG&E cannot agree the modifications are cost effective since the work to complete the implementation of the CIP-013-1 set of Standards is just being completed and full testing has not been completed to determine the cost of that work. As noted in the PG&E input on the first Comment & Ballot for these modifications, PG&E would have preferred to have an "Unknown" option to select.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Do not agree. Tri-State contends that the edits should have been risk-based and only applicable to the control portions of PACS and EACMS, and not also the monitoring portions of those systems. Additionally, time and resources would be saved if the SDT would include language that clarifies that entity-initiated remote access and entity-initiated vendor remote access are not prohibited by CIP standards.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EACMS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Although ISO-NE acknowledges the importance of establishing Supply Chain requirements associated with EACMS and PACS, ISO-NE respectfully believes that it cannot clearly determine if the modified requirements would meet the FERC directives in a cost effective manner because the current CIP-005-6, CIP-010-3 and CIP-013-1 standards have yet to become effective. It is difficult to determine cost-effectiveness when the approach is to build on requirements that the Industry has had limited experience with and limited opportunities for lessons learned or to mature processes and controls.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	No

Document Name	
Comment	
"vendor-initiate remote access" only seems to apply to R3 of CIP-005-7, so the summary above does not accurately reflect the changes to R2 of CIP-005-7. "Vendor Initiated" should be included in CIP-007 R2.4 and 2.5. Leaving non-vendor initiated remote access in R2.4 and R2.5 is purely administrative in nature. SMUD has implemented this requirement as it is currently written and have found it to be both operationally inefficient and lacking value from a security standpoint. For R3, this question cannot be answered because it is unclear what constitutes an authenticated vendor-initiated remote connection.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts. The SDT recommends reviewing the Technical Rationale, which states the below: • A 'connection' is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating. • "Authentication" is the mechanism for the EACMS or PACS to identify the user or device. • This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to 'how' authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment
To minimize churn among standard versions and better identify the scope, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-005-7, CIP-010-4, and CIP-013-2 with other existing drafting teams for related standards; specifically, Projects 2016-02, 2020-03, and 2020-04. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see the response at the beginning of question 4.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment
BC Hydro recommends changing the applicability around PACS to be associated with Medium Impact BCS with ERC instead of just Medium Impact BCS to avoid confusion. The modifications under CIP-010-4 R1.6 to include PACS associated with Medium Impact BES Cyber Systems is otherwise out of alignment in regards to the application of PACS under the CIP standards. The CIP standards under CIP-006-6 require the application of PACS in environments associated with High Impact BES Cyber Systems, Medium Impact BES Cyber Systems with External Routable Connectivity, and associated EACMS and PCAs but do not require this for Medium Impact BES Cyber Systems *without* ERC. By expanding the requirement and application of PACS to Medium Impact BES Cyber Systems without any qualifier per CIP-010-4 R1.6, it is not clear whether this is implied to bring into scope similar or identical cyber assets to PACS that may be used by

entities to restrict and/or monitor access to Medium Impact without ERC BES Cyber Systems but which would not meet the definition of PACS (even though the application of these are not required by the standards).	
Likes 0	
Dislikes 0	
Response Thank you for your comment. PACS are not currently required for medium impact BES Cyber Systems without External Routable Connectivity. Furthermore, all requirements in CIP-010-4 are subject to the text in the "Applicable Systems" at the beginning of the standard which states "Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity."	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The basic capability of detecting (which is a better term than determine) remote session activity is the relevant security control. Whether that activity is initiated by a vendor, partner, customer, or an employee is irrelevant to the technical capability. Scoping the requirement narrowly does not provide significant cost savings and still allows for poor security. BPA does not agree with feedback that monitoring for remote sessions by employees could be a union issue. There is a difference between monitoring for external sessions vs monitoring employee activity within a session and this requirement does not go that far. Insider threat remains the number one threat to critical infrastructure and the ability to actively detect and terminate a session regardless of who originates it is a key cyber security control.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. FERC Order 850 and the drafting team SAR, directed the SDT to modify the standard to specifically deal with vendors, any additions to the standard language would be considered outside the scope of the SAR.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST recommends modifying proposed changes to CIP-005, as per our response to Question 1.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response is question 1.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
please reference Marty Hostler, Northern California Power Agency, comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to Northern California Power Agency.	
Andrea Barclay - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	

GSOC agrees that the SDT has worked to fine tune requirements to ensure security and cost-effectiveness. However, GSOC remains concerned about the scope of EACMSs to which the requirements are applicable and how the current scope increases the overall cost and burden on registered entities. For these reasons, GSOC recommends that the SDT work on additional fine-tuning of the overall scope of applicability as related to EACMSs.

Additionally, GSOC notes that the multiple requirements, "interchangeable" terms, and potential for confusion and ambiguity detract from the potential cost-effectiveness of these standards. The elimination of multiple, "interchangeable" terms through the use of definitions and defined terms along with streamlined requirements will help to further fine-tune the scope and security obligations set forth within these standards. They will also facilitate consistent, effective compliance auditing, making these reliability standards more cost-effective across the ERO Enterprise.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your response, however, at this time there is no separation of access control vs. monitoring within the approved definition of EACMS and the SDT must use approved definitions. Additionally, a change to the definition of EACMS is outside the SAR for this SDT due to EACMS being used throughout the CIP standards, and only CIP-005, CIP-010 and CIP-013 are open for this SDT. The SDT considered adding qualifying language to the standard such as "EACMS, excluding those that provide only monitoring and logging", however, this change could introduce the requirement of maintaining "lists" of EACMS and what functions they provide.

Marty Hostler - Northern California Power Agency - 5

Answer	Yes
Document Name	
Comment	

Cost effective is vague. Please provide a cost/benefit justification for any posposed changes.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Janet OBrien - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with comments submitted separately by Tom Breene of WEC	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to WECC.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We recommend defining the term 'Vendor Initiated Remote Access', and define who is considered a vendor.	

Likes 0	
Dislikes 0	
Response Thank you for your response. Vendor is not a defined term, however as written by the original Project 2016-03 SDT and included in the CIP-013-2 Technical Rationale "The term vendor(s) as used in the standard is limited to those persons, companies, or otherorganizations with whom the Responsible Entity, or its affiliates, contract with to supply BESCyber Systems and related services. It does not include other NERC registered entities providingreliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant toNERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers ormanufacturers of information systems, system components, or information system services; (ii)product resellers; or (iii) system integrators."	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ray Jasicki - Xcel Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tony Skourtas - Los Angeles Department of Water and Power - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits. In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see the response at the beginning of question 4.	
Becky Webb - Exelon - 6	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	
While the IRC SRC acknowledges that EACMS and PACS are important to protect and believes it is good business practice to apply supply chain security controls to all Cyber Assets in the enterprise, it also believes that regulatory compliance has the potential to increase the cost of implementation and maintenance. At times, this can be dramatic, to a point where it may be detrimental to a company's overall security posture, thereby ultimately increasing the security risk to the company. NERC and the industry should continue to monitor and evaluate cost versus security benefits. In that regard, the IRC SRC proposes that after CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years, NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard. This will allow for the processes and controls to mature and for Reliability Entities to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the response at the beginning of question 4.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
No comment on cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy sees potential schedule and cost risks in implementing yet to be defined tools.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	

5. Provide any additional comments for the standard drafting team to consider, if desired.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	

Answer	
Document Name	
Comment	
The wording in CIP-013 R1.2.6 should match the wording in CIP-005-7 R3 P3.2, to wit: “authenticated vendor-initiated remote connections”	
Likes 0	
Dislikes 0	
Response Thank you for your comment. CIP-005-7 Requirements R3.1 and 3.2 include very specific prescriptive language for “authenticated vendor-initiated remote connections.” However, CIP-013-2 requires the entity to develop a plan to address vendor risk, and therefore the phrase “vendor-initiated remote access” included in requirement R1.2.6 does not need to be as specific or prescriptive, and each entity will determine which vendors are in scope.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

The SDT uses the term “sessions” in CIP-005-7 R2 but in CIP-005-7 R3, it proposes replacing the term “session” with “connection.” Since there is no definition of “connection” in the *Glossary of Terms Used in NERC Reliability Standards* or in the NIST online glossary, BPA believes the term “connection” is ambiguous and should not be used within the standard.

Proposed change to CIP-005-7 R3.1:

Have one or more method(s) for detecting remote access sessions.

Proposed change to CIP-005-7 R3.2:

Have one or more method(s) for terminating remote access sessions.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT recommends reviewing the Technical Rationale, which states the below:

- A ‘connection’ is the mechanism for a user or a system to interact with an EACMS or PACS for the purpose of authenticating.
- “Authentication" is the mechanism for the EACMS or PACS to identify the user or device.
- This identification of the user or device permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections in order to come to a determination on applicability for Part 3.1. It is very important to note, this new proposed language is not prescriptive as to ‘how’ authentication must occur in order to permit the entity to implement whatever administrative and/or technical methods work in their environment.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	
Comment	
Further clarity should be provided regarding the definition of “vendor” in relation to staff augmentation consultants/contractors who may performing system integration work or supporting/managing the operation of BES Cyber Assets via remote access. NERC had during CIP-013-1 standard development responses to industry, indicated that it does not consider staff augmentation contractors/consultants who are treated similar to employees to be considered vendors. However, WECC is communicating a different approach in compliance outreach sessions and are expecting entities to identify staff augmentation contractors/consultants to be considered as vendors due to risks they could pose. This should be clarified within the standards to either allow entities the flexibility to define who vendors are to them ***or*** to have the standard drafting team define this clearly through a proposed Glossary defined term or within the standard language itself as the current definition within the standard is open to interpretation between enforcement entities and create undue compliance burden.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has provided guidance in Technical Rationale which states “The term vendor(s) as used in the standard is limited to those persons, companies, or otherorganizations with whom the Responsible Entity, or its affiliates, contract with to supply BESCyber Systems and related services. It does not include other NERC registered entities providingreliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant toNERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers ormanufacturers of information systems, system components, or information system services; (ii)product resellers; or (iii) system integrators.” The SDT urges Registered Entities to submit larger concerns of inconsistent interpretation through NERC’s Consistency Reporting Tool to enter the ERO Enterprise Program Alignment Process led by NERC’s Compliance & Enforcement team, who can assess and unify audit interpretation.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment	
In regards to CIP-010-4 Requirement 1 Part 1.6, PCAs should also be included in the Applicable Systems. When BES Cyber Systems and PCAs are located within the same ESP and software is validated and verified for the BCS but not the PCAs, a mixed-trust security environment is created within an ESP. By not including PACs in the Applicable Systems, it poses additional unnecessary risk to the security of the BES.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The NERC Supply Chain report did not recommend including PCAs at this time.	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
The language is very clear in this version.	
Likes 0	
Dislikes 0	
Response Thank you for your comment.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	

Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Based on industry comment, the SDT determined that an 18 month implementation plan was appropriate.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E has no additional input regarding this Comment & Ballot.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	

MEC supports EEI comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Neil Shockey - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI's comments	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Regarding the Implementation Guidance for CIP-005-7, we provide the following four (4) comments:

(1) Page 3, 2nd paragraph - Suggest adding 'within the Electronic Security Perimeter' as EACMS can reside within the ESP and this appears to be the context of these EACMS.

(2) 'However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS,'

Change to "However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS within the Electronic Security Perimeter,[…]"

(3) Page 5, 2b 'Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture'

Suggest different wording than architecture. Perhaps network topology?

(4) Page 7 - While this section contains a “cut and paste” of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is from the CIP-005-6 standard, consider detailing the first use of EAP as it isn't used anywhere prior in the IG. Change 'Responsible Entities should know what traffic needs to cross an EAP' to "Responsible Entities should know what traffic needs to cross an Electronic Access Point (EAP)..."

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT has taken these comments into consideration and modified the Implementation Guidance based on comments 1-3. The section of the GTB that is cut and paste from CIP-005-6 will remain intact in its historical version.

Jose Avendano Mora - Edison International - Southern California Edison Company - 1

Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-03 Supply Chain Risks	
Answer	
Document Name	
Comment	
The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The standards were balloted together as they are collectively referred to as the supply chain risk management Reliability Standards per FERC Order 850. The SDT choose to ballot all the standards together to ensure they all passed industry approval to meet the deadline in FERC Order 850.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	

Document Name	
Comment	
We appreciate the SDT efforts.	
Likes 0	
Dislikes 0	
Response Thank you for your response.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Marcus Moor, Westar Energy, 1, 5, 3, 6; Thomas ROBBEN, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	

Comment	
Westar Energy and Kansas City Power & Light, the Evergy companies, support and incorporate by reference the Edison Electric Institute's response to Question 5.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. Please see response to EEI.	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	

In the Technical Rationale for Reliability Standard CIP-013-2 document (page 11), “Requirement R2” should read “Requirement R3”. The text indicates “The proposed requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P.46) “. R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The Technical Rational for CIP-013-2 Page 11 is the historical section preserving the CIP-013-1 Technical Rationale. This has been corrected in the main body of the document.

Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	

Comment
The CAISO supports the ISO/RTO Council Standards Review Committee comments below. The IRC SRC requests the SDT create individual ballots for each standard included in this project. This would provide flexibility to the industry to support certain aspects of this project while expressing concerns over other aspects.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The standards were balloted together as they are collectively referred to as the supply chain risk management Reliability Standards per FERC Order 850. The SDT choose to ballot all the standards together to ensure they all passed industry approval to meet the deadline in FERC Order 850.

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Comments from EEI

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments: While EEI supports the changes made by the SDT, which addressed prior EEI member comments related to CIP-005-7 Requirement R2 Parts 2.4 and 2.5, we recommend the SDT revise "vendor remote access" to "vendor initiated remote access" or explain why all vendor remote access needs to be evaluated for Parts 2.4 and 2.5.

   EEI supports the current proposed draft language for Requirement R3.

   Response: Thank you for your comments. In response to industry comments from the former ballot, the SDT decided to revert Parts 2.4 and 2.5 to the original FERC approved language to resolve the recursive issues and refocused on the FERC directives, NERC recommendation, and the SAR by creating self-contained Requirement R3. This new requirement is mutually exclusive from R2 and its parts.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry's concerns about recursive requirements ('hall of mirrors'). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments: EEI supports the changes made by the SDT to address prior EEI member comments related to the "hall of mirrors" issue.

Response: Thank you for your comment.

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments:

   Response:

4. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner by fine tuning the scope of the modified requirements to vendor-initiated remote access. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments: EEI has no comment on the cost effectiveness of the proposed changes.

   Response: Thank you for your response.

5. Provide any additional comments for the standard drafting team to consider, if desired.

   Comments: EEI previously provided comments that CIP-005-7 did not provide sufficient clarity regarding contractors who are essential to the reliable operation of the BES. Specifically, the Reliability Standard did not provide a mechanism that exempted contractors who provided essential contract services. Although CIP-005-7 does not explicitly provide a defined process for exempting these contractors, the draft Implementation guidance makes it clear that these types of contractors are to be handled in a manner similar to the staff of a registered entity.

   Response: Thank you for your comment.

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2019-03 Cyber Security Supply Chain Risks

Additional Ballot and Non-binding Poll Open through September 10, 2020

Now Available

The additional ballot and non-binding poll are open through **8 p.m. Eastern, Thursday, September 10, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

The standard drafting team's considerations of the responses received from the last comment period are reflected in these drafts of the standards.

Balloting

Use the Standards Balloting and Commenting System (SBS) to submit votes. Contact Wendy Muller regarding issues using the SBS.

Note: Votes cast in the previous ballot will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to vote again in the additional ballot. NERC asks those not wanting to vote affirmative or negative cast an abstention to ensure a quorum is reached.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-03 Cyber Security Supply Chain Risks Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Formal Comment Period Open through September 10, 2020

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Thursday, September 10, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

The standard drafting team's considerations of the responses received from the last comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standards and implementation plan as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **September 1-10, 2020**.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify "Project 2019-03 Cyber Security Supply Chain Risks Observer List" in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/203)
Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 AB 3 ST
Voting Start Date: 9/1/2020 12:01:00 AM
Voting End Date: 9/10/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 243
Total Ballot Pool: 306
Quorum: 79.41
Quorum Established Date: 9/10/2020 4:22:59 PM
Weighted Segment Value: 80.78

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	81	1	53	0.828	11	0.172	1	3	13
Segment: 2	6	0.6	4	0.4	2	0.2	0	0	0
Segment: 3	68	1	43	0.843	8	0.157	1	2	14
Segment: 4	20	1	10	0.714	4	0.286	0	0	6
Segment: 5	72	1	46	0.852	8	0.148	2	1	15
Segment: 6	48	1	27	0.871	4	0.129	1	1	15
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	1	0.1	0	0	0	2	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	1	0	0	0	0	0	0	1	0
Segment: 10	7	0.5	4	0.4	1	0.1	1	1	0
Totals:	306	6.2	188	5.008	38	1.192	6	11	63

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Renee Leidel		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		None	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Evergy	Allen Klassen		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Troy Hlavaty		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	No Comment Submitted
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		None	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Third-Party Comments
1	Puget Sound Energy, Inc.	Chelsey Neil		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		None	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Allen Klassen		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Jamie Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		None	N/A
3	Eversource Energy	Christopher McKinnon		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	No Comment Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PSEG - Public Service Electric and Gas Co.	maria pardo		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		None	N/A
3	Seattle City Light	Laurie Hammack		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	Joel Dembowski		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Marcus Moor		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Austin Energy	Jun Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	None	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Scott Tomashefsky		None	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Avani Pandya	Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Neil Shockey		Affirmative	N/A
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Evergy	Derek Brown		None	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	No Comment Submitted
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NaturEner USA, LLC	Spencer Weiss		None	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Shivaz Chopra		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	No Comment Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		None	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		None	N/A
5	Seattle City Light	Faz Kasraie		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Affirmative	N/A
5	Westar Energy	Derek Brown		Affirmative	N/A
6	AEP	JT Kuehne		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Colorado Springs Utilities	Melissa Brown		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Evergy	Thomas ROBBEN		None	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
6	Florida Municipal Power Pool	Aaron Casto	Truong Le	None	N/A
6	Great River Energy	Donna Stephenson		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Nick Burns		Negative	No Comment Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Marty Watson		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation	Ron Carlsen		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Thomas ROBBEN		Affirmative	N/A
6	Western Area Power Administration	Erin Green		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
8	David Kiguel	David Kiguel		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Negative	No Comment Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 306 of 306 entries

BALLOT RESULTS

Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 Non-binding Poll AB 3 NB
Voting Start Date: 9/1/2020 12:01:00 AM
Voting End Date: 9/10/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 223
Total Ballot Pool: 290
Quorum: 76.9
Quorum Established Date: 9/10/2020 4:41:42 PM
Weighted Segment Value: 76.97

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	74	1	37	0.755	12	0.245	12	13
Segment: 2	6	0.4	3	0.3	1	0.1	2	0
Segment: 3	67	1	34	0.791	9	0.209	9	15
Segment: 4	16	1	7	0.636	4	0.364	1	4
Segment: 5	70	1	34	0.773	10	0.227	9	17
Segment: 6	46	1	17	0.773	5	0.227	6	18
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	1	0.1	0	0	2	0
Segment: 9	1	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	3	0
Totals:	290	5.9	137	4.528	41	1.372	45	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		None	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Jose Avendano Mora		None	N/A
1	Evergy	Allen Klassen		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Troy Hlavaty		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	None	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		None	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Chelsey Neil		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Matt Carden		None	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Allen Klassen		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Affirmative	N/A
2	California ISO	Jamie Johnson		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		None	N/A
3	Eversource Energy	Christopher McKinnon		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	maria pardo		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		None	N/A
3	Seattle City Light	Laurie Hammack		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Marcus Moor		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	None	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Avani Pandya	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	mark brewer		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Affirmative	N/A
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Evergy	Derek Brown		None	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NaturEner USA, LLC	Spencer Weiss		None	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		None	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		None	N/A
5	Seattle City Light	Faz Kasraie		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Affirmative	N/A
5	Westar Energy	Derek Brown		Affirmative	N/A
6	AEP	JT Kuehne		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Colorado Springs Utilities	Melissa Brown		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Evergy	Thomas ROBBEN		None	N/A
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Carey		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
6	Florida Municipal Power Pool	Aaron Casto	Truong Le	None	N/A
6	Great River Energy	Donna Stephenson		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Muscatine Power and Water	Nick Burns		Negative	Comments Submitted
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Marty Watson		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Thomas ROBBEN		Affirmative	N/A
6	Western Area Power Administration	Erin Green		Affirmative	N/A
8	David Kiguel	David Kiguel		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 290 of 290 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standards for a formal 10-day comment and ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ final draft of the proposed standards for a formal ~~45~~10-day comment and ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
~~45-day formal comment period with second additional ballot~~	~~July 28 – September 10, 2020~~
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEAmay ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			to-system remote access) (2.5).	(2.5).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standards for a formal 10-day comment and ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~6~~7

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~6~~7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-~~6~~7 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-~~6~~7 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~6~~7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to determine authenticated vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method to determine authenticated vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan for Project 2019-03
- CIP-005-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated:	Authorize and document changes that deviate from the existing baseline	Examples of evidence may include, but are not limited to:

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	configuration.	• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	and their associated: 1. EACMS; 2. PACS; and 3. PCA	1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~final draft of proposed standard for formal ~~45~~10-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
~~45-day formal comment period with second additional ballot~~	~~July 28 – September 10, 2020~~
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Date: See Implementation Plan for Project 2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated:	Authorize and document changes that deviate from the existing baseline	Examples of evidence may include, but are not limited to:

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	configuration.	• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	and their associated: 1. EACMS; 2. PACS; and 3. PCA	1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-~~3~~4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~3~~4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-~~5.1~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS;	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to:

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA		• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	and their associated: 1. EACMS; 2. PACS; and 3. PCA	1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment,	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including ~~of~~ the date of the test.

CIP-010-~~3~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		including a description of the measures used to account for any differences in operation between the test and production environments.	
1.6	High Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and ~~1.~~2. PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~3~~4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

~~None.~~

- Implementation Plan for Project 2019-03.
- CIP-010-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised

Version	Date	Action	Change Tracking
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	

CIP-010-~~3~~4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-~~3~~4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1:- Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating

the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
~~45-day formal comment period with second additional ballot~~	~~July 28 – September 10, 2020~~
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, ~~-~~as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	February 20, 2019
SAR posted for comment	February 25 – March 27, 2019
45-day formal comment period with ballot	January – March 2020
45-day formal comment period with additional ballot	May 7 – June 22, 2020
45-day formal comment period with second additional ballot	July 28 – September 10, 2020

Anticipated Actions	Date
10-day final ballot	October 2020
Board adoption	November 2020

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-~~1~~2**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-~~1~~2:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002~~-5,~~ or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project ~~2016~~2019-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems~~.~~ and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for ~~(i)~~ vendor-initiated ~~Interactive Remote Access, and (ii) system-to-system~~ remote access ~~with a vendor(s).~~.

M1. Evidence shall include~~-~~ one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber ~~systems~~Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- ~~Link to the~~ Implementation Plan ~~and other important associated documents.~~ for Project 2019-03
- CIP-013-2 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
~~Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).~~2	TBD	Modified to address directive in FERC Order No. 850.	

~~Rationale~~

~~Requirement R1:~~

~~The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):~~

~~(1) Software integrity and authenticity;~~
~~(2) Vendor remote access;~~
~~(3) Information system planning; and~~
~~(4) Vendor risk management and procurement controls.~~

~~The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.~~

~~Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).~~

~~Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.~~

~~Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.~~

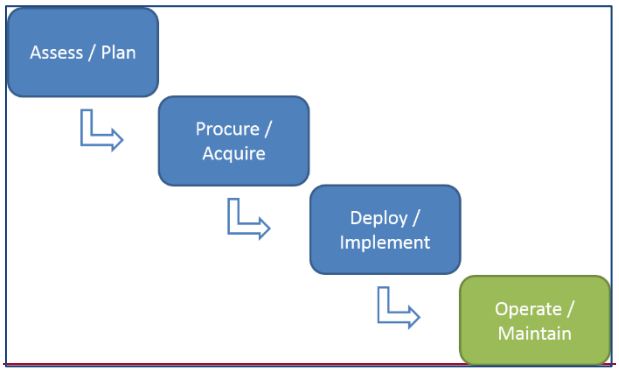
~~The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the~~

~~awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.~~

~~The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.~~

~~Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.~~

~~Notional BES Cyber System Life Cycle~~



~~Requirement R2:~~

~~The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).~~

~~Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:~~

- ~~NERC or the E-ISAC~~
- ~~ICS-CERT~~
- ~~Canadian Cyber Incident Response Centre (CCIRC)~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6[1]. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber

[1] In the event CIP-002-6 has not yet been approved or otherwise made effective in the applicable jurisdiction, please refer to the Implementation Plan associated with CIP-002-5.1a.

System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-03 Cyber Security Supply Chain Risks

Applicable Standard(s)

- CIP-005-7 — Cyber Security — Electronic Security Perimeters
- CIP-010-4 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-2 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

- CIP-005-6 — Cyber Security — Electronic Security Perimeters
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-013-1 — Cyber Security — Supply Chain Risk Management

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

For all Reliability Standards in Project 2019-03 — CIP-005-7, CIP-010-4, and CIP-013-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in Reliability Standards CIP-010-4 and CIP-013-2 as follows:

- CIP-010-4, Requirement R2, Part 2.1: within 35 calendar days of the Responsible Entity's last performance of Requirement R2, Part 2.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.1: within 15 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.1 under CIP-010-3.
- CIP-010-4, Requirement R3, Part 3.2: within 36 calendar months of the Responsible Entity's last performance of Requirement R3, Part 3.2 under CIP-010-3.
- CIP-013-2, Requirement R3: on or before the effective date of CIP-013-2.

Planned or Unplanned Changes

Compliance timelines with CIP-005-7, CIP-010-4, and CIP-013-2 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with CIP-002-6[1]. The Implementation Plan associated with CIP-002-6 provides as follows:

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-6, Attachment 1, then the new BES Cyber

[1] In the event CIP-002-6 has not yet been approved or otherwise made effective in the applicable jurisdiction, please refer to the Implementation Plan associated with CIP-002-5.1a.

System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation. For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the responsible entity and subsequently identified through the annual assessment under CIP-002-6, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-6, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-6, Attachment 1, criteria.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies its first high impact or medium impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-6 identification and categorization processes)	24 months

Retirement Date

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 shall be retired immediately prior to the effective date of Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-005-7, Requirements R1 and R2

The VRFs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirements R1 and R2

The VSLs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2

The VRFs for all requirements in CIP-013-2 did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirements R1 and R2

The VSLs did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirements.

VSL Justification for CIP-013-2, Requirement R3

The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method to authenticate vendor-initiated remote connections for PACS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate established vendor-initiated remote connections for PACS (3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method for detecting vendor-initiated remote connections for EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
		method to terminate authenticated vendor-initiated remote connections for EACMS (3.2).	

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium for Requirement R3, which addresses Vendor Remote Access Management for EACMS and PACS, is consistent with Reliability Standard CIP-005-7 Requirement R2, which addresses Remote Access Management and includes requirements for vendor access management for high and certain medium impact BES Cyber Systems and associated PCA.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser-risk reliability objective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system for supply chain requirements. Proposed CIP-005-7 Requirement R3 is a new requirement that includes methods to determine and terminate authenticated vendor-initiated remote connections for EACMS, which is similar to requirements in Parts 2.4 and 2.5 for other applicable systems. Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	NERC – Cyber Security Supply Chain Risks, Chapter 2	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system for supply chain requirements. Proposed CIP-005-7 Requirement R3 is a new requirement that requires processes that include methods to determine and terminate authenticated vendor-initiated remote connections for PACS, which is similar to requirements in Parts 2.4 and 2.5 for other applicable systems.

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system for supply chain requirements. ~~These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements.~~ Proposed CIP-005-7 Requirement R3 is a new requirement that includes methods to determine and terminate authenticated vendor-initiated remote connections for EACMS, which is similar to requirements ~~Parts 3.1 and 3.2 in CIP-005-7 were previously located~~ in Parts 2.4 and 2.5 for other applicable systems. ~~in CIP-005-6, and include modifications from the language used in CIP-005-6.~~ Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the	NERC – Cyber Security Supply Chain	The SDT proposed the modified language in CIP-005-7 Requirement R3and CIP-010-4 Requirement R1.6 to include PACS as an applicable system for supply chain requirements. ~~These requirements are the supply chain requirements~~

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
scope of the supply chain risk management Reliability Standards.	Risks, Chapter 2	~~embedded in the CIP-005 and CIP-010 requirements.~~ Proposed CIP-005-7 Requirement R3 is a new requirement that requires processes that include methods to determine and terminate authenticated vendor-initiated remote connections for PACS, which is similar to requirements ~~Parts 3.1 and 3.2 in CIP-005-7 were previously located~~ in Parts 2.4 and 2.5 for other applicable systems. ~~in CIP-005-6, and include modifications from the language used in CIP-005-6.~~ Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-7 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7.

To address industry concern during the second ballot regarding the required use of Intermediate Systems and EACMS, and the creation of a 'hall of mirrors', the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. To further address industry concern, references to Interactive Remote Access (IRA) and the undefined term system to system were removed.

The table shows the current approved CIP-005-6 as compared to the final draft posting of CIP-005-7.

Current approved CIP-005-6 Language	CIP-005-7 Language – Current Posting
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
	Requirement R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS.* [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
	Requirement R3, Part 3.1: Have one or more method(s) to determine authenticated vendor-initiated remote connections.
	Requirement R3, Part 3.2: Have one or more method(s) to terminate authenticated vendor-initiated remote connections sessions and control the ability to reconnect.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-4 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-010-4.

To address the FERC directives, EACMS and PACS were added to the Applicable Systems for Requirement R1 Part 1.6. No modifications have been made to the requirement language itself.

The table shows the current approved CIP-010-3 as compared to the final draftposting of CIP-010-4.

Current approved CIP-010-3 Language	CIP-010-4 Language – Current Posting
Requirement R1 Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	**Requirement R1 Part 1.6:** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-013-2 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-013-2.

To address the FERC directives, EACMS and PACS were added to Requirements R1 and R2. To address industry concern during the second ballot regarding 'hall of mirrors' for EACMS and the required use of Intermediate Systems, as well as concerns about inconsistencies in language between procurement planning requirements in CIP-013-2 and the operational security requirements of CIP-005-7, references to Interactive Remote Access (IRA) and the undefined term system to system were removed from, CIP-013-2 Requirement R1.2.6, because authenticated remote connections and system to system remote connections for EACMS and PACS; and IRA and system to system access to BCS and PCAs are all sub-types of vendor-initiated remote access.

The table shows the current approved CIP-013-1 as compared to the final draft posting of CIP-013-2.

Current approved CIP-013-1 Language	CIP-013-2 Language – Current Posting
Requirement R1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*	**Requirement R1:** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
Requirement R1.1: One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	**Requirement R1.1:** One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
Requirement R1.2: One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:	**Requirement R1.2:** One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:
Requirement R1.2.5:	**Requirement R1.2.5:**

Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and
Requirement R1.2.6: Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	**Requirement R1.2.6:** Coordination of controls for (i) vendor-initiated ~~Interactive R~~remote ~~A~~access~~, and (ii) system-to-system remote access with a vendor(s)~~.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

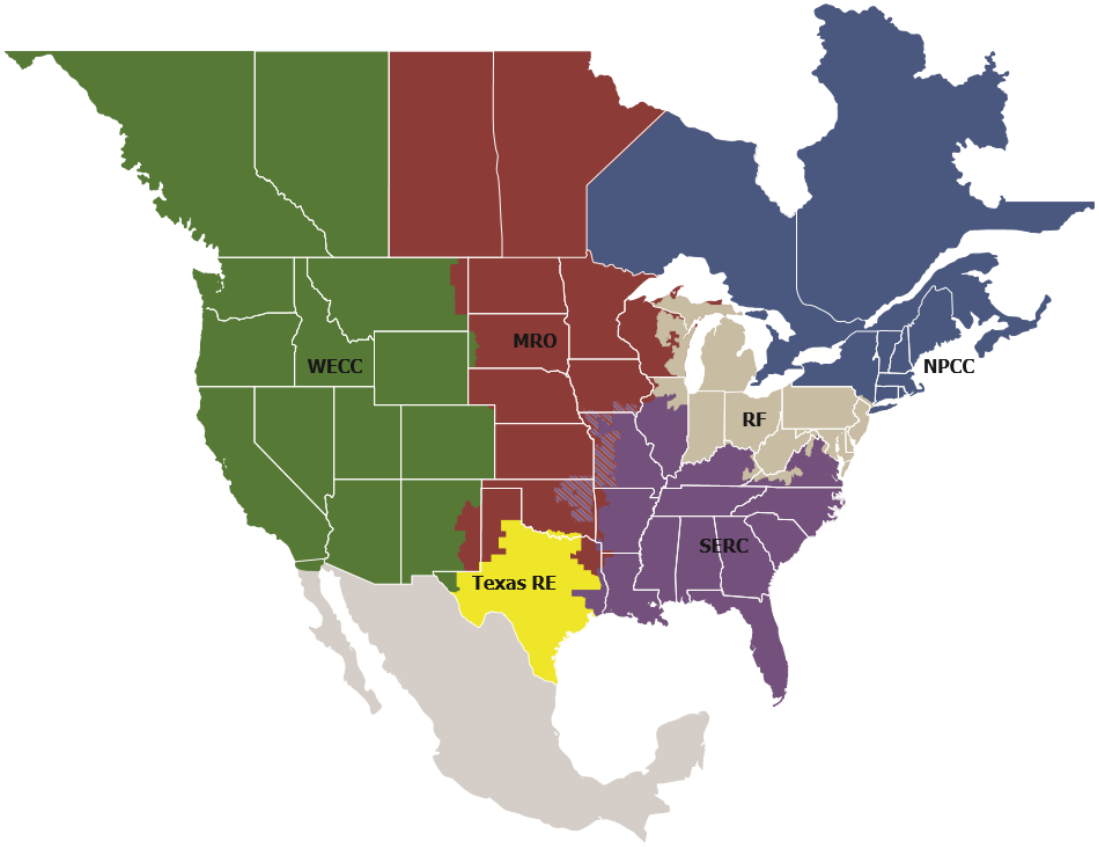
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement 1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the "first line of defense within an Industry Control System (ICS) network environment". The compromise of those devices that control access management could provide an outsider the "keys to the front door" of the ESP where BES Cyber Systems reside. An intruder holding the "keys to the front door" could use those "keys" to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and

3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

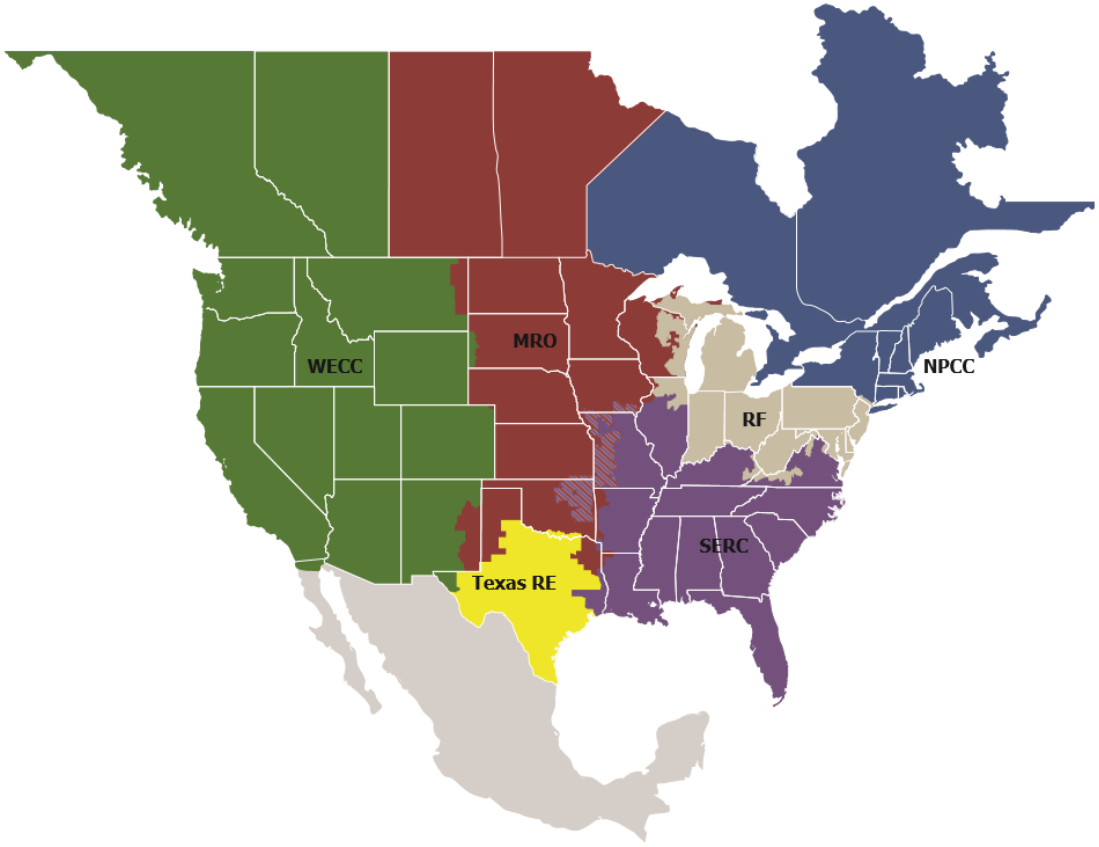
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the

cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient

device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-2

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

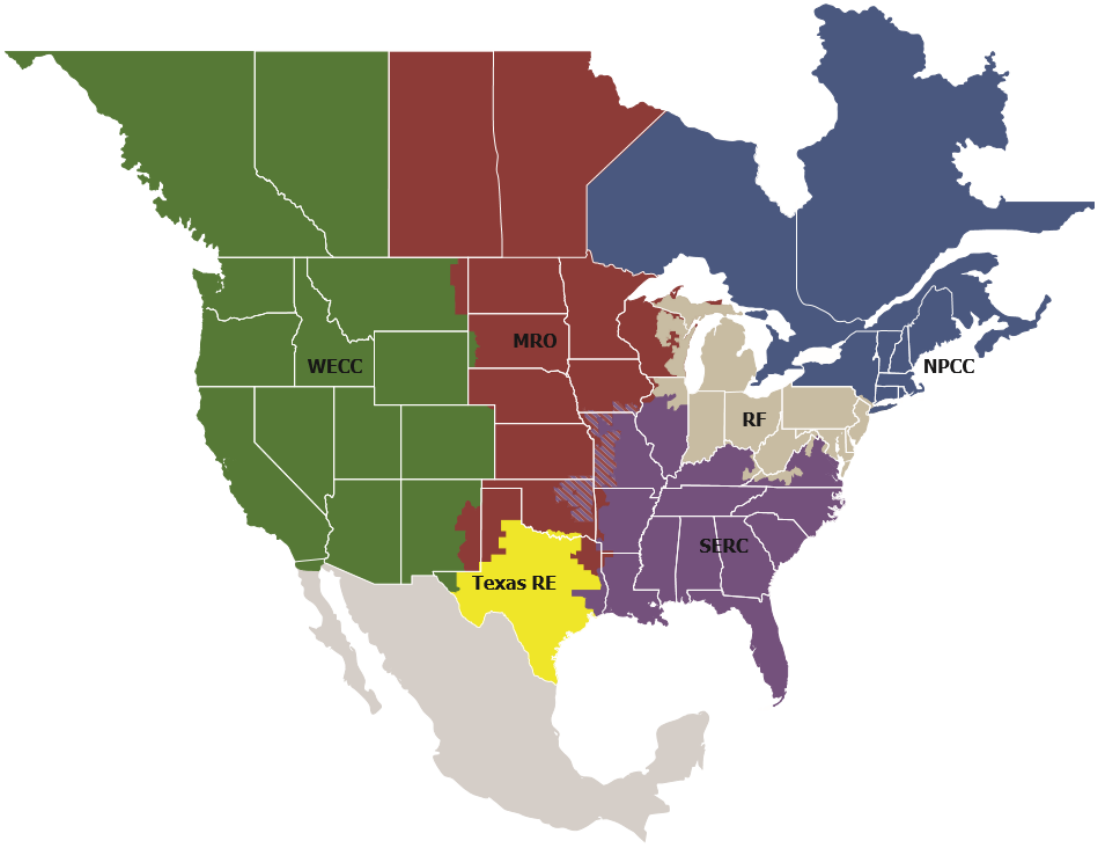
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

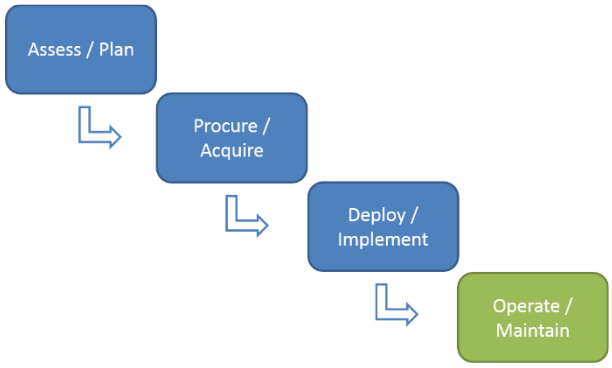
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

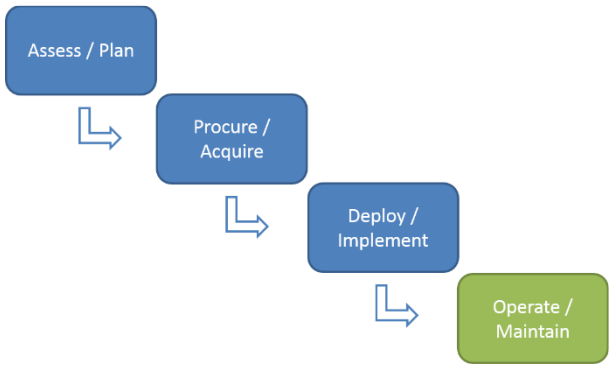
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

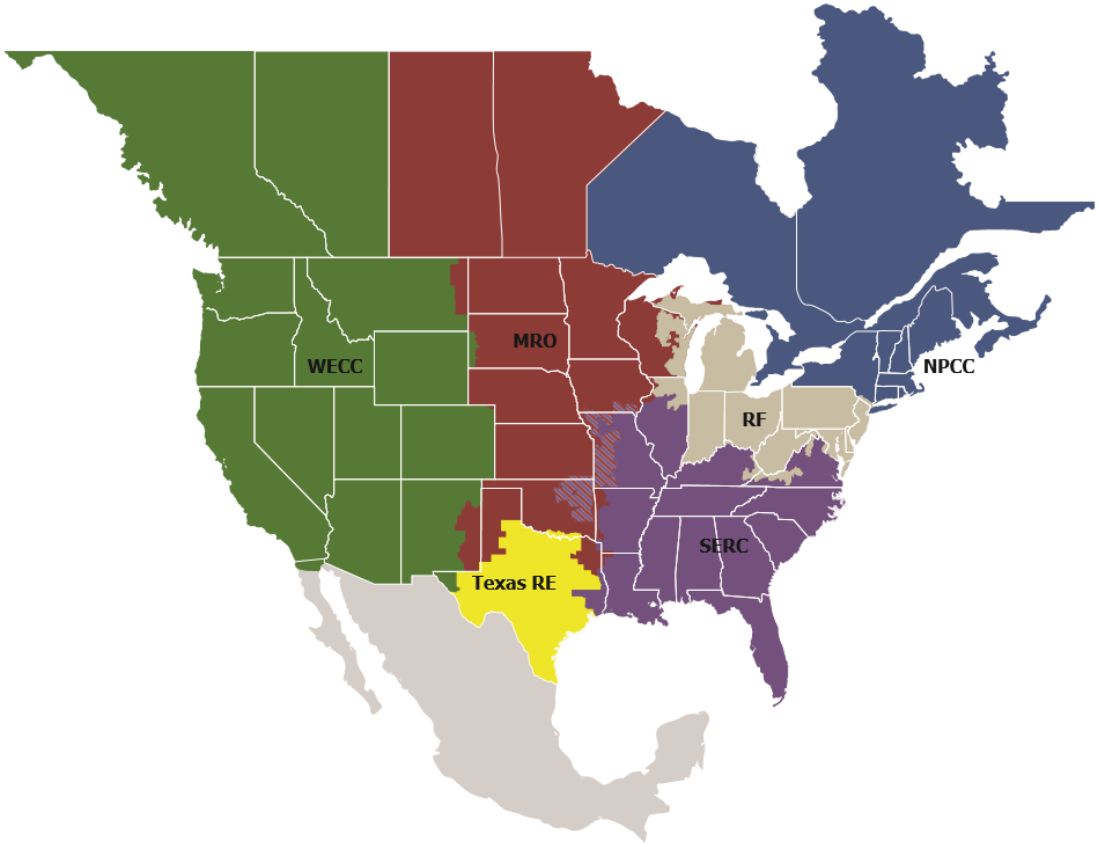
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements Parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method to determine authenticated vendor-initiated remote connections is documented and the ability to disable that remote connection is required. For example, if an entity utilizes its corporate remote access solution to allow remote connection into its PACS, the entity would need to document the authenticated remote connection method and develop a process to terminate such connections after authentication. Some examples of how an entity might terminate these connections may be as simple as, but are not limited to actions like disabling a token or certificate for a vendor account(s), suspending or deleting the vendor account(s) in Active Directory, blocking the vendor's IP range, or physically disconnecting a network cable.

Intermediate Systems (a subset of EACMS) use is not a requirement for remote access to other EACMS, lessening the potential of the recursive requirement ("hall of mirrors") However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS (within the Electronic Security Perimeter), the process of terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor attempts the remote access connection, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable the vendor's ability to make a connection. The remote access vendor will attempt to "connect" with the EACMS however, after unsuccessful authentication the connection attempt will be terminated. This scenario illustrates a method to disallow vendor-initiated remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and network topologies to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes

to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

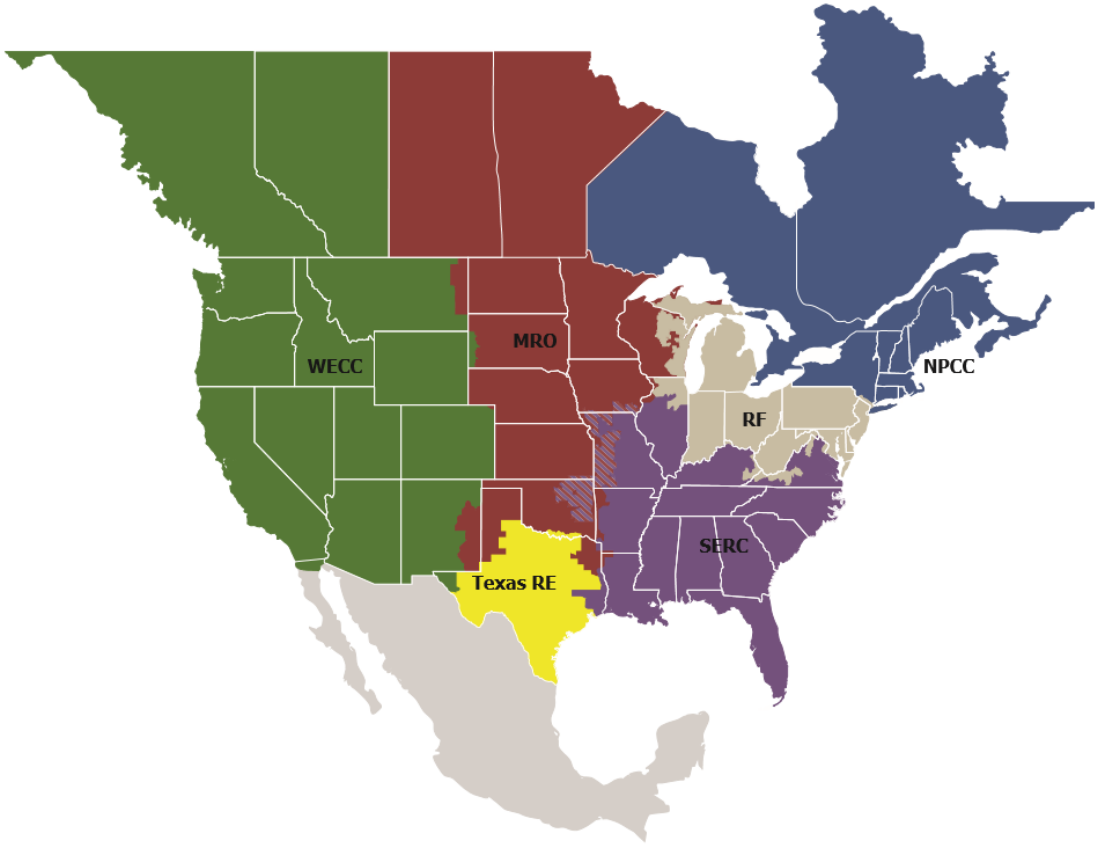
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements Parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. If an entity allows remote access to their EACMS and PACS the method to determine authenticated vendor-initiated remote connections is documented and the ability to disable that remote connection is required. For example, if an entity utilizes its corporate remote access solution to allow remote connection into its PACS, the entity would need to document the authenticated remote connection method and develop a process to terminate such connections after authentication. Some examples of how an entity might terminate these connections may be as simple as, but are not limited to actions like disabling a token or certificate for a vendor account(s), suspending or deleting the vendor account(s) in Active Directory, blocking the vendor's IP range, or physically disconnecting a network cable.

Intermediate Systems (a subset of EACMS) use is not a requirement for remote access to other EACMS, lessening the potential of the recursive requirement ("hall of mirrors") However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS (within the Electronic Security Perimeter), the process of terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor attempts the remote access connection, the jump host will present both the Active Directory login screen as well as the multifactor access portal. The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable the vendor's ability to make a connection. The remote access vendor will attempt to "connect" with the EACMS however, after unsuccessful authentication the connection attempt will be terminated. This scenario illustrates a method to disallow vendor-initiated remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and network topologies ~~architecture~~ to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.
    c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.
    d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4 Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes

to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4 Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security — Configuration Change Management and Vulnerability Assessments

Implementation Guidance for Reliability Standard CIP-010-4

October 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

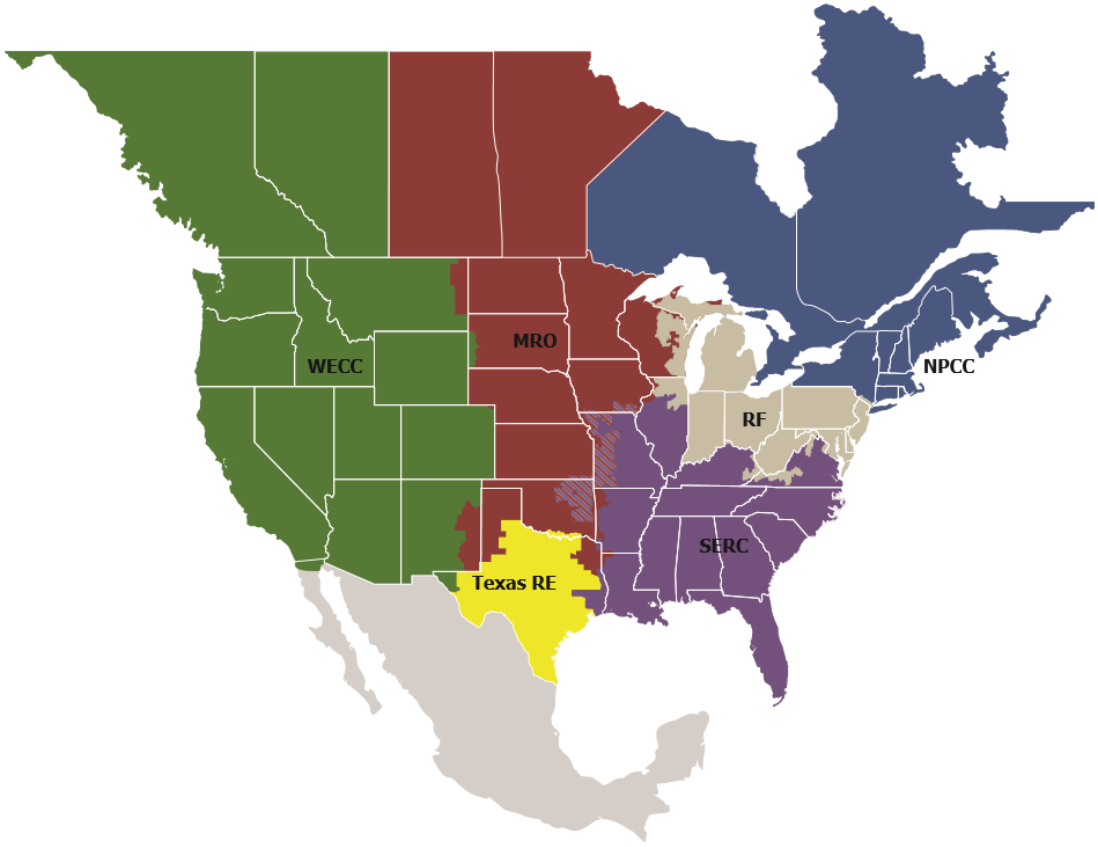
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-010-4. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides one or more examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-010-4.

This document is composed of approaches written by previous drafting teams, relevant to previous versions of CIP-010, as well as additions by the Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) related to the modifications. Anything relevant to version 4 of this standard that was written by previous SDT's is included in this document.

Project 2019-03 was initiated due to the Federal Energy Regulatory Commission (the Commission) issuing Order No. 850[2] on October 18, 2018, in which the summary on page 1 states, "…the Comission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[3], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT modified Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

[2] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[3] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

General Considerations for Requirement R1 Part 1.5

Test Environment

The Responsible Entity should note that wherever a test environment (or the test is performed in production in a manner that minimizes adverse effects) is mentioned, entities are required to "model" the baseline configuration and not duplicate it exactly.

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

General Considerations for Requirement R1 Part 1.6

Software Verification

NIST SP-800-161 includes a number of security controls, which together reduce the probability of a successful "Watering Hole" or similar cyber-attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires information systems prevent the installation of firmware or software without digital signature verification so genuine and valid hardware and software components are used. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify and validate digital signature on the software to detect modifications indication compromise of the software's integrity.
- Use public key infrastructure (PKI) with encryption as a method to prevent software modification in transit by enabling only intended recipients to decrypt the software.
- Require fingerprints or cipher hashes from software sources for all software and compare the values to the authoritative source prior to installation on a BES Cyber System as verification of the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Even after verification is completed, it is still recommended that software testing is performed. If the integrity and authenticity checks are only performed at vendor point of origin, there is no guarantee that the product being retrieved is untainted prior to availability at the point of origin. The vendor checks performed do not detect embedded malicious code in the software, firmware or patch between the vendor applying the integrity method and the implementation of the software by the Registered Entity on a high or medium impact BES Cyber System and its associated EACMS or PACS.

Implementation Guidance for R1

Refer to ERO Enterprise Endorsed Implementation Guidance document CIP-010-3 R1.6 Software Integrity and Authenticity for additional compliance guidance and examples etc.

Implementation Guidance for CIP-010-3

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

None

Requirement R1:

Baseline Configuration

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

None

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the

information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

<u>Per Transient Cyber Asset Capability</u>

For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.2: To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014[4]. Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

[4] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Entities should also consider whether the detected malicious code is a Cyber Security Incident.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for Reliability Standard CIP-013-2

October 2020

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

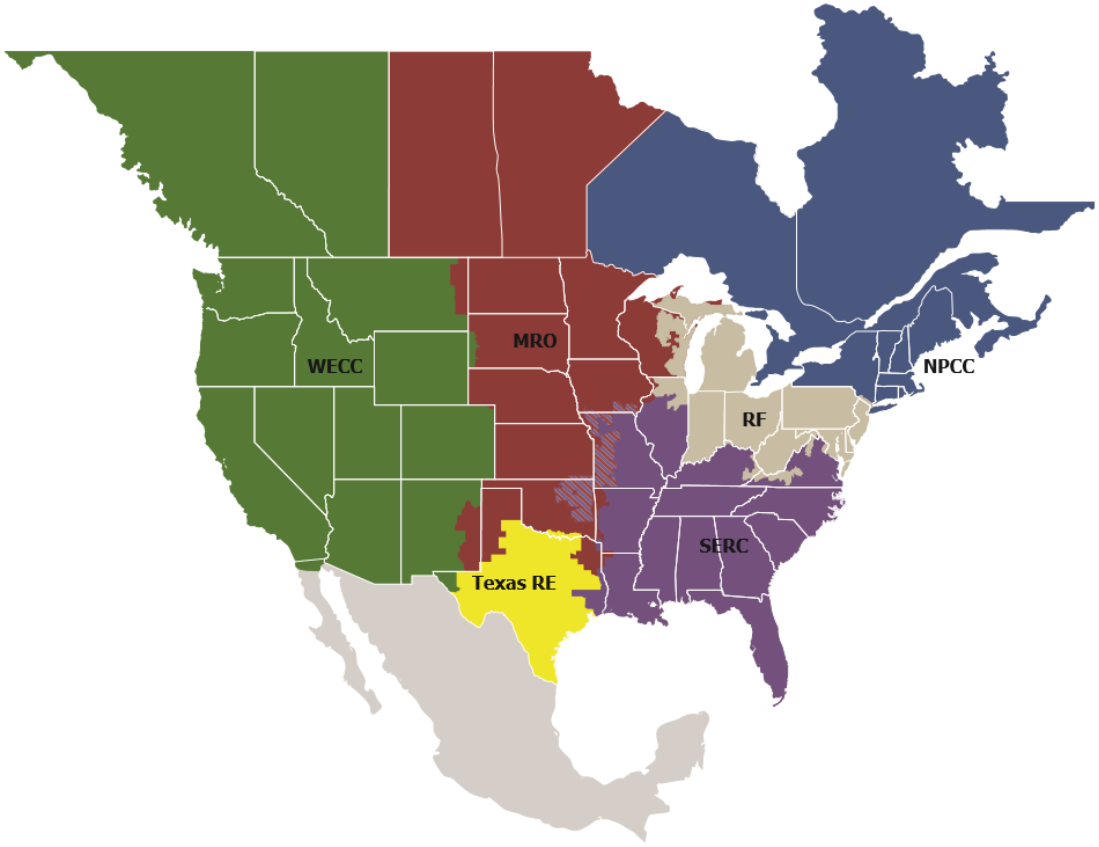
Table of Contents

Preface

*Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. T*he vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1] and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

1.2.6. *Coordination of controls for vendor-initiated remote access.*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-2.

> *Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.*

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

  1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review)

approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:
    - Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
    - Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

1.2.5. *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-2. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2.

Requirement R3

R3. *Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) "Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation"
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-03 Cyber Security Supply Chain Risks

Final Ballot Open through October 16, 2020

Now Available

The final ballot is open through **8 p.m. Eastern, Friday, October 16, 2020** for the following:

- CIP-005-7 – Cyber Security - Electronic Security Perimeter(s)
- CIP-010-4 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-013-2 – Cyber Security - Supply Chain Risk Management
- Implementation Plan

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pool(s) associated with this project can log in and submit their votes here. Contact Wendy Muller regarding issues using the SBS.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standards will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2019-03 Cyber Security Supply Chain Risks CIP-005-7, CIP-010-4, & CIP-013-2 FN 4 ST
Voting Start Date: 10/7/2020 12:02:01 PM
Voting End Date: 10/16/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 4
Total # Votes: 249
Total Ballot Pool: 298
Quorum: 83.56
Quorum Established Date: 10/7/2020 4:39:15 PM
Weighted Segment Value: 76.76

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	54	0.794	14	0.206	0	3	9
Segment: 2	6	0.6	4	0.4	2	0.2	0	0	0
Segment: 3	67	1	43	0.811	10	0.189	0	2	12
Segment: 4	20	1	10	0.714	4	0.286	0	0	6
Segment: 5	69	1	45	0.804	11	0.196	0	2	11
Segment: 6	45	1	26	0.813	6	0.188	0	2	11
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	3	0.1	1	0.1	0	0	0	2	0
Segment: 9	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.6	4	0.4	2	0.2	0	1	0
Totals:	298	6.3	187	4.836	49	1.464	0	13	49

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	City Water, Light and Power of Springfield, IL	Chris Daniels		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	N/A
1	Dairyland Power Cooperative	Renee Leidel		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		None	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Troy Hlavaty		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		None	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	N/A
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		None	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Jamie Johnson		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Colleen Campbell		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	Intermountain REA	Pam Feuerstein		None	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Trevor Tidwell		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	maria pardo		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A
3	Seattle City Light	Laurie Hammack		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Jun Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	None	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	N/A
4	Northern California Power Agency	Scott Tomashefsky		None	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Avani Pandya	Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	mark brewer		Negative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Affirmative	N/A
5	Enel Green Power	Mat Bunch		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NaturEner USA, LLC	Spencer Weiss		None	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Shivaz Chopra		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Mahmood Safi		None	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	Seattle City Light	Faz Kasraie		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Affirmative	N/A
6	AEP	JT Kuehne		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Abstain	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Colorado Springs Utilities	Melissa Brown		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
6	Florida Municipal Power Pool	Aaron Casto	Truong Le	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Nick Burns		Negative	N/A
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Joe Tarantino	Negative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Santee Cooper	Marty Watson		Negative	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Western Area Power Administration	Erin Green		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
8	David Kiguel	David Kiguel		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Negative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit I

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2109-03 Cyber Security Supply Chain Risks

April 1, 2020

	Name	Entity
Chair	JoAnn Murphy	PJM Interconnection L.L.C.
Vice Chair	Tony Hall	LG&E and KU Energy
Members	Howard Hunt	Southern Company
	Jeffery Sweet	American Electric Power (AEP)
	Sharon Koller	American Transmission Company, LLC
	Jason Snodgrass	Georgia Transmission Corp
	Brian Gayle	Dominion Energy, Inc.
	John Hargrove	John Hargrove PE-TX Technology Consulting
PMOS Liaison(s)	Kirk Rosener	CPS Energy
	Linda Lynch	FPL
NERC Staff	Alison Oswald – Senior Standards Developer	North American Electric Reliability Corporation
	Marisa Hecht – Senior Counsel	North American Electric Reliability Corporation