UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RM24-8-000**
	)	

ERRATA AND SUPPLEMENTAL PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

Lauren Perotti
Assistant General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

May 20, 2025

TABLE OF CONTENTS

Exhibits Proposed Reliability Standards

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RM24-8-000**
	)	

ERRATA AND SUPPLEMENTAL PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

The North American Electric Reliability Corporation ("NERC")[1] hereby submits errata to five proposed Reliability Standards and supplemental information to the petition for approval of Critical Infrastructure Protection ("CIP") Reliability Standards submitted on July 10, 2024 in the aforementioned docket (hereinafter referred to as "Original Petition").[2]

The errata are to the following proposed Reliability Standards:

- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-011-4 - Cyber Security – Information Protection

In addition, NERC submits clarifications to the redline versions of proposed Reliability Standards CIP-003-10 and CIP-011-4 submitted as part of the Original Petition to better illustrate the changes from previously Commission-approved Reliability Standards. [3] Finally, given the extensive record

[1] The Federal Energy Regulatory Commission ("FERC" or "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) *order on reh'g & compliance,* 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC,* 564 F.3d 1342 (D.C. Cir. 2009).

[2] *Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection Reliability Standards*, Docket No. RM24-8-000 (July 10, 2024).

[3] Unless otherwise indicated, all capitalized terms used in this petition shall have the meaning set forth in the Glossary of Terms used in NERC Reliability Standards ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

within the Original Petition, NERC further highlights record excerpts containing the justification for some technical concepts within the proposed Reliability Standards.

As provided in the Original Petition, industry stakeholders have identified the need for the CIP Reliability Standards to enable adoption of newer technologies in a secure manner. To that end, the proposed Reliability Standards use language with security objectives, which not only facilitates virtualization but also further supports adoption of emerging technology to help ensure the resilience of operation technology. Specifically, objective-based requirements focus Responsible Entities[4] on what they need to achieve and not necessarily how they need to achieve it, helping to ensure that the CIP Reliability Standards can swiftly adapt to new security technology and Responsible Entities can quickly change methods or technologies to adapt to evolving risks without the immediate need to revise Reliability Standards. Accordingly, NERC respectfully requests the Commission approve the proposed Reliability Standards in the Original Petition, and as amended in the instant filing, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also reiterates its request for approval of the following in the Original Petition: (1) four new and 18 proposed revised definitions; (2) the associated Implementation Plan; (3) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs"); and (4) the retirement of the currently effective versions of several CIP Reliability Standards.[5]

I. ERRATA

Subsequent to the filing of the Original Petition, NERC became aware of an error in referencing the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems columns of some of the proposed Reliability Standards. In those proposed

[4] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

[5] NERC is requesting the retirement of CIP-002-5.1.a, CIP-003-9, CIP-004-7, CIP-005-7, CIP-006-6, CIP-007-6, CIP-008-6, CIP-009-6, CIP-010-4, CIP-011-3, and CIP-013-2.

Reliability Standards, the first use of the term incorrectly is stated as "Electronic Access Control *and* Monitoring System (EACMS)" [emphasis added] instead of the correct term "Electronic Access Control *or* Monitoring System (EACMS)" [emphasis added]. This error appears in the following proposed Reliability Standards requirement parts:

- CIP-006-7 Requirement R1, Part 1.2
- CIP-007-7 Requirement R1, Part 1.1
- CIP-008-7 Requirement R1, Part 1.1
- CIP-009-7 Requirement R1, Part 1.1
- CIP-011-4 Requirement R1, Part 1.1

At its meeting on April 16, 2025, the Standards Committee approved the errata under Section 12.0 of Appendix 3A to the NERC Rules of Procedure, Standard Processes Manual,[6] indicating the Standard Committee's agreement that the correction (1) does not change the scope or intent of the Reliability Standards and (2) the correction has no material impact on the end users of the Reliability Standard.[7] Under NERC's standards numbering system,[8] the errata standards' version numbers add a ".1" to the version number that was filed with the Original Petition. The errata are included in Exhibits 2 through 6 to this petition. NERC respectfully requests that the Commission approve the proposed Reliability Standards CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, and CIP-011-4.1 included in Exhibits 2 through 6 in lieu of proposed Reliability

[6] The NERC Rules of Procedure, including Appendix 3A, NERC Standard Processes Manual, are available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

[7] Under Section 12.0: Process for Correcting Errata in the NERC Rules of Procedure, Appendix 3A (Standard Processes Manual), errors may be corrected in a Reliability Standard: (i) following a Final Ballot prior to Board of Trustees adoption, (ii) following Board of Trustees adoption prior to filing with Applicable Governmental Authorities; and (iii) following filing with Applicable Governmental Authorities. If the Standards Committee agrees that the correction of the error does not change the scope or intent of the associated Reliability Standard, and agrees that the correction has no material impact on the end users of the Reliability Standard, then the correction shall be filed for approval with Applicable Governmental Authorities as appropriate. The NERC Board of Trustees has resolved to concurrently approve any errata approved by the Standards Committee.

[8] NERC Standards Numbering System (May 22, 2023), https://www.nerc.com/pa/Stand/Resources/Documents/NERC%20Standards%20Numbering%20System.pdf.

Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7, and CIP-011-4 included in Exhibit A of the Original Petition.

II. REDLINE CORRECTIONS

NERC also identified three instances where the redlines filed in the Original Petition did not reflect all changes made across standard versions: two instances in the redline version of proposed Reliability Standard CIP-003-10 submitted in Exhibit A-2 to the Original Petition and one instance in the redline version of CIP-011-4 submitted in Exhibit A-10 to the Original Petition. NERC filed these redline versions to demonstrate the changes in proposed CIP-003-10 and CIP-011-4 against the last versions of those standards approved by the Commission. The clean versions of the Reliability Standards and the redline versions of the Reliability Standards properly demonstrate the proposed Reliability Standards language. Therefore, NERC is not submitting errata versions of these proposed Reliability Standards. In the interest of providing a full and complete record for the Commission's consideration, however, NERC clarifies the aspects in which the redlines filed in the Original Petition failed to demonstrate all of the changes across versions. The updated redline of proposed CIP-003-10 is included in this petition as Exhibit 1, and the updated redline of proposed CIP-011-4.1 is included in Exhibit 6.

First, the redline version of proposed CIP-003-10 does not show the addition of the acronym for BES Cyber System, which is BCS, in redline as reflecting a change across versions. This first use of the defined term BES Cyber Systems appears in the purpose statement of the standard, which is not considered one of the "enforceable" sections of the Reliability Standard. Therefore, the purpose in the redline of CIP-003-10 should read as follows, with "BCS" in blackline:

> To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber

> Systems **(BCS)** against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

The second instance is in Section 5.2.1 of Attachment 1 to proposed Reliability Standard CIP-003-10. The redline version does not show deleted language that was in CIP-003-9. The bullets in Section 5.2.1 provide a non-exhaustive list of methods for Responsible Entities to meet the security objective of mitigating the risk of introduction of malicious code to low impact BES Cyber Systems for Transient Cyber Assets managed by a party other than the Responsible Entity. The following language should be shown as deleted in the bullets of Section 5.2.1 (in blackline):

- ~~Review use of live operating system and software executable only from read-only media;~~

The drafting team determined to remove the bullet as it is a more prescriptive description of the methods to mitigate the risk of introduction of malicious code, but Responsible Entities may still use the deleted method to achieve the objective of the requirement as it is captured in the last bullet of the proposed requirement as an "other method."

For proposed Reliability Standard CIP-011-4, the redline version does not show that Requirement R2, Part 2.2 of Reliability Standard CIP-011-3 was deleted. Accordingly, the redline in Exhibit A-10 to the Original Petition should show 2.2 deleted as follows (in blackline):

~~2.2~~	~~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~~	~~Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence may include, but are not limited to, the following:~~ • ~~Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ • ~~Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.~~

As noted in the technical rationale for CIP-011-4 in Exhibit E-10 to the Original Petition, Requirement R2, Part 2.2 from CIP-011-3 was consolidated into Part 2.1 of proposed Reliability Standard CIP-011-4 through objective-level requirement language. The drafting team noted that this consolidation is necessary to enable flexibility, allowing for cryptographic erasure in scenarios where BES Cyber System Information cannot be mapped to one or more disks within a virtualized storage cluster, and where BES Cyber System Information is stored on Cyber Systems employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned or managed by a third-party as a service to the entity for its BES Cyber System Information storage, analysis, or use.

III. SUPPLEMENTAL INFORMATION ON JUSTIFICATION FOR PROPOSED RELIABILITY STANDARDS

As noted in the Original Petition, the proposed standards and definitions improve upon the current standards and definitions by further refining the requirements' focus on cyber security through: (1) the use of objectives to permit use of a broader variety of security controls tailored to

an organization's technologies, (2) revision of requirements that focused more on compliance documentation, and (3) clarification of issues identified during implementation of prior versions of CIP Reliability Standards.

Through the use of security objectives in requirement language, the proposed Reliability Standards accommodate more than just a perimeter-based network security model and enable the requirements to better accommodate virtualized environments as well as future technologies. In so doing, the proposed Reliability Standards update a suite of Reliability Standards that include some concepts that have been relatively unchanged for over two decades,[9] even though technology used in industrial control systems has advanced rapidly within that timeframe. While these proposed revisions were necessary to better accommodate today's technology (e.g., virtualized environments, etc.), they also reflect the principle that the CIP Reliability Standards should not hinder a Responsible Entity from implementing new technology securely. As a result, the use of security objectives enhances reliability of the Bulk Power System ("BPS") by focusing the requirement language on *what* a Responsible Entity should achieve in implementing security controls but not *specifically how* it should implement it, regardless of whether the Responsible Entity continues to use perimeter-based network security models, virtualized technologies, or a combination thereof.

Additionally, by shifting the focus from documentation in some requirements to the security objective a Responsible Entity shall achieve, the proposed Reliability Standards enhance the reliability of the BPS. For example, while Responsible Entities may continue to use, and expand the use of, a baseline to meet the configuration change management requirements in

[9] In the Urgent Action 1200 standard in 2003, the primary focus was the "critical cyber asset," an "electronic device" such as a server, workstation, or relay as a physical object. Similarly, in the currently enforceable CIP Reliability Standards, a Cyber Asset relies upon an asset having its own physical hardware. With virtualization, physical devices are no longer the primary units of organization.

proposed Reliability Standard CIP-010-5, the security objective language also permits Responsible Entities to authorize intended changes to certain security controls in a forward-looking manner. Such an approach can be more appropriate for an environment using automation, virtualization, or both, ensuring dynamic virtual machines would be, for example, automatically patched upon instantiation. Accordingly, the proposed revisions do not let the documentation inherent to a baseline configuration impede Responsible Entities from leveraging a security solution that could better accommodate the dynamic nature of virtualization.

Finally, as noted in the Original Petition, the proposed Reliability Standards support reliability of the BPS by clarifying concepts that NERC, the Regional Entities, and Responsible Entities identified during implementation of prior versions of the CIP Reliability Standards, including Interactive Remote Access, CIP Exceptional Circumstances, and Technical Feasibility Exceptions.[10] Developing such revisions in response to input from implementation is a key component of the compliance-standards feedback loop in promoting revisions to Reliability Standards that enhance reliability of the BPS.

Given the extensive record included with the Original Petition, NERC highlights the below excerpts from the record to assist the Commission with navigating the breadth of information justifying the proposed Reliability Standards. The following sections include excerpts from the technical rationale documents included as Exhibits to the Original Petition that reflect the technical justification for the revisions. Section III.A. addresses the revised approach to electronic access control; Section III.B. addresses the revised approach to ports and services management; Section III.C. addresses the revised approach to configuration change management; and Section III.D. addresses some of the new proposed terms.

[10] Technical Feasibility Exceptions are defined in Appendix 2 to the NERC Rules of Procedure, https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix%202%20eff%2020240627_signed.pdf.

A. Revised Approach to Electronic Access Control

Proposed Reliability Standard CIP-005-8 provides objective level requirements around electronic access controls to medium and high impact BES Cyber Systems and their Protected Cyber Assets. As stated in the Original Petition,

> [p]roposed Requirement R1, Part 1.2 removes an explicit requirement to use an Electronic Access Point to control communications to applicable systems but replaces it with core security objectives of permitting "only needed routable communications" through the Electronic Security Perimeter and denying all others (excluding time sensitive communications of Protection Systems). This security objective focuses on the "reachability" of applicable systems, permitting Responsible Entities to use Electronic Access Points to control the accessibility of the applicable systems, among other controls.[11]

In addition, the Original Petition referenced Exhibit E-4, which provides technical rationale regarding the revisions in proposed CIP-005-8.[12] The drafting team underwent thoughtful deliberations when developing the technical rationale to support the proposed language revisions, particularly when developing revisions in response to industry stakeholders. Specifically, the following excerpt from Exhibit E-4 to the Original Petition provides information on how the security objective would be achieved in implementing zero-trust architecture or a perimeter-based network security model, or both, demonstrating that all ingress and egress access points through the Electronic Security Perimeter would be defined under the revised approach to electronic access controls. This excerpt also discusses the types of time-sensitive communications of Protection Systems that are excluded from Requirement R1, Part 1.2, including the purpose behind the revisions in CIP-005-8 in enabling Responsible Entities to implement the security controls that are most appropriate for their organization's technology:

---

[11] Original Petition at p. 41.
[12] Original Petition at p. 45.

[Proposed Requirement R1, Part 1.2] changed to a security objective, rather than prescribing [External Routable Connectivity] must be controlled at an [Electronic Access Point]. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened [Electronic Security Perimeter (ESP)] definition are flexible in how the objective is met.

The intent of "through the ESP" is to better incorporate future Zero Trust implementations where there is no "logical border surrounding a network" but instead Policy Enforcement Points at the accessed resource itself or as close to it as possible. In these instances that are designed to be perimeter-less, the concepts of "inside" and "outside" begin to fail and the [drafting team] is removing those now to be better prepared for future technologies. The [drafting team] asserts that even in traditional Layer 3 firewalls that define an ESP, the communications between systems that are encapsulated in packets go "through" the perimeter (ESP) in order to reach their destination.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the 'reachability' of the Applicable Systems; filtering network communications before they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

…

> Additionally, within the Measures, the [drafting team] uses examples of VLAN and VXLAN configurations as evidence. These configurations could be used as methods to "Permit only needed routable protocol communications", despite not being OSI layer routable protocols in and of themselves.
>
> Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols are excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The [drafting team] intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.[13]

This excerpt highlights that Responsible Entities may continue to use perimeter-based models to meet the security objective of Requirement R1. The objective-level language also permits Responsible Entities to leverage other security controls, such as a policy enforcement point. Therefore, while the proposed Reliability Standard no longer limits Responsible Entities to using a perimeter-based model, Responsible Entities may continue to meet the security objective of the requirement by deploying such a configuration.

The proposed revisions to the definitions of Electronic Security Perimeter and Electronic Access Point are used within Requirement R1 of CIP-005-8. As with all terms within the NERC Glossary, understanding those definitions is essential to implement Requirement R1. Below is an

[13] Original Petition Exhibit E-4 at pp. 8-9.

excerpt from Exhibit E-12 to the Original Petition where the drafting team described various configurations of an Electronic Security Perimeter and Electronic Access Points:

> The [Electronic Security Perimeter] definition was modified to provide flexibility and the use of various architectures and access control models. The traditional network border [Electronic Security Perimeter] remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed [Electronic Security Perimeter] definition retains its current definition but appends "or a logical boundary defined by one or more [Electronic Access Point]s" to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a [BES Cyber System]. The proposed definition allows for an [Electronic Security Perimeter] to be (a) a border surrounding an isolated network that has no external connectivity and thus no [Electronic Access Point]s, (b) static point(s) on a network boundary such as a traditional firewall as an [Electronic Access Point] that is enforcing access policies or configurations (e.g., firewall rulesets), (c) many dynamic, short-lived, session-level 'perimeters' established at time of access that are network independent (e.g., users to resources, for example), or (d) hybrid implementations combining elements of more than one model.
>
> The [drafting team] has kept the 'logical border' concept for the "surrounding a network" [Electronic Security Perimeter] and used the language "logical boundary" for zero trust models. A 'border' does indeed surround an object, in this case a network, but a 'boundary' may not surround or enclose, it's a line that can be crossed, such as a policy enforcement point controlling access to a resource. The [drafting team] has also updated language in the standards to remove concepts such as 'inside' an [Electronic Security Perimeter] and replaced that with more inclusive phrases such as 'protected by' an [Electronic Security Perimeter].[14]
> …
> As network security moves deeper into the infrastructure, it's no longer necessary to prescribe that network security be performed only at a 'Cyber Asset interface on an [Electronic Security Perimeter]' at one point on a network edge. Zero Trust, for example,

[14] Original Petition Exhibit E-12 at pp. 4-5.

> highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of "electronic policy enforcement point or" [into the Electronic Access Point definition]. With the added flexibility in CIP-005 to adopt these models in addition to the traditional [Electronic Security Perimeter] model, the [Electronic Access Point] definition was modified to allow for electronic policy enforcement points and no longer prescribes an architecture. The "one or more" and the "associated [Protected Cyber Asset]s" have been added to clarify that [Electronic Access Point]s can control communications to a group and [are] not required per individual system.[15]

These excerpts provide examples of various ways a Responsible Entity would implement proposed CIP-005-8 Requirement R1 electronic access control requirements. Regardless of how each Responsible Entity chooses to implement the revised requirements, the ERO Enterprise will assess through its CMEP activities whether Responsible Entities are implementing the proposed Reliability Standards in a consistent and secure manner that is appropriate for each configuration and meets the security objective of the requirement.

B. Revised Approach to Ports and Services Management

Proposed Reliability Standard CIP-007-7 specifies technical, operational, and procedural requirements to manage system security (e.g., malicious code prevention methods, patch management, etc.). As stated in the Original Petition,

> proposed Requirement R1, Part 1.1 changes its focus from enabling or restricting ports to the broader focus of disabling or preventing unneeded routable protocol network accessibility. In some instances, a Responsible Entity may be able to disable a service or remove or uninstall software that is providing unneeded network accessibility to the applicable system. In other instances, a Responsible Entity may not be able to disable a service but can prevent access to it in another layer, such as the underlying operating system with a host-based firewall, a policy enforcement point, or other means of filtering traffic.[16]

---

15 Original Petition Exhibit E-12 at p. 4.

16 Original Petition at p. 46.

Under this approach, Responsible Entities may continue to manage system security by enabling only logical network accessible ports that have been determined to be needed by the Responsible Entity as is required under the currently effective Reliability Standard CIP-007-6, but may also adopt broader approaches, such as a "user to tagged workload" level access control policy at a different OSI level, among others that meet the intent of the objective. The following language is an excerpt from the technical rationale from Exhibit E-6 that provides additional context behind the security objective language in the proposed revisions in CIP-007-7:

> Requirement R1 Part 1.1 requires "disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability". The [drafting team] updated the Requirement Part language to state a security objective concerning "*routable protocol network accessibility*" as opposed to "ports and services". As this is a new phrase, the intent of this phrase with some examples and rationale for this change is as follows.
>
> The objective of [the] phrase [routable protocol network accessibility] in the Requirement [R1] Part [1.1] is to reduce the attack surface on an applicable system by preventing any unnecessary accessibility to the system over a network using routable protocols. "Accessibility" as used in [Part] 1.1 is at the routable protocol network level and does not include physical access, logon to the physical console, code on [Transient Cyber Assets or Removable Media], etc. Port numbers [(Transmission Control Protocol/User Datagram Protocol)] are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, reducing network accessibility in the physical underlay of [Shared Cyber Infrastructure] between hypervisors or on fabric-based networks may be best performed at a *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server [Virtual Cyber Asset], it may be easier to show that network accessibility on that [Virtual Cyber Asset] is limited to SQL server and remote admin enabled port numbers. In Zero Trust Architectures (ZTA), it may be neither ports or services, but instead a "user to tagged

workload" level access control policy where accessibility is described and protected at a more granular, yet higher level than a port #, enforced at a Policy Enforcement Point (PEP) on the applicable system. The [drafting team] has moved to this objective language to avoid prescribing only one way to perform and document network accessibility in all these various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part. The objective is to know the ways a system can be accessed from the network via routable protocols and have no unnecessary attack surface from that perspective.

In this Requirement [R1] Part [1.1], the [drafting team] used the verbs "Disable or prevent". In some cases, the entity may be able to disable a service or remove/uninstall software that is providing unneeded network accessibility to the applicable system. In other cases, the entity may not be able to disable a service, but can prevent access to it in another layer, such as the underlying OS with a host-based firewall, a PEP, or other means of filtering traffic. In instances where the entity can do neither (e.g., a firmware-based 'black box' device with limited configuration capabilities), the [drafting team] chose to add 'per system capability' to make the requirement conditional on the ability of the applicable system to meet it, if the entity can show that it is incapable.

The [drafting team] also added the clarifier "on each Applicable System" to indicate that the intent of this requirement is for an entity to perform the configuration actions ***on*** each Applicable System, hardening the system from its routable protocol network peers rather than having a single method such as an [Electronic Access Point] network firewall rule that would disable such accessibility for a group of Applicable Systems on a network. In other words, merely filtering a port/service on a firewall at an [Electronic Security Perimeter] network boundary (CIP-005 R1 controls) does not meet the intent of CIP-007 R1.[17]

[17] Original Petition at Exhibit E-6, pp. 4-6.

With these revisions, proposed CIP-007-7 supports reliability by focusing Responsible Entities on hardening their systems against unneeded network accessibility. In fact, the proposed Reliability Standard raises the security bar as Responsible Entities need to understand the ways in which each system is "listening" (i.e. can be accessed) so that the Responsible Entity disables or prevents any accessibility that is not needed rather than only the typical ports and services. While that is still a method to meet the security objective, other methods also may be used to ensure the Responsible Entity meets the security objective.

C. Revised Approach to Configuration Change Management

Proposed CIP-010-5 governs change management requirements and vulnerability assessment requirements for medium and high impact BES Cyber Systems. As stated in the Original Petition,

> proposed [CIP-010-5] Requirement R1 focuses on authorizing intended changes that alter security behaviors rather than focusing on listing and documenting changes. In a dynamic environment such as virtualization, where a Virtual Cyber Asset may lie dormant but automatically patched at a future instantiation, the goal of change management is to ensure any changes are authorized prior to that instantiation, not tracking the time and date when the patching occurs for each instantiation with an update to the baseline 30 days later. As a result, the focus of proposed Requirement R1 has changed from documenting the installed software and its open ports on a Cyber Asset or Virtual Cyber Asset at some point post-change to authorizing the changes that will occur when it does instantiate, which provides more security value for virtualized environments.[18]

The proposed revisions broaden the change management requirements by incorporating the security objective of controlling the implementation of intended changes to software or settings that could weaken certain cyber security controls rather than only permitting a baseline configuration. Responsible Entities may continue to use a baseline configuration to meet the

[18] Original Petition at p. 49.

requirements of proposed CIP-010-5, but the changes that will be managed are more focused on how controls behave.

The following excerpt from the technical rationale from Exhibit E-9 provides additional information on the approach behind the security objective in the proposed revisions in CIP-010-5:

> In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS or firmware, installed and custom software, ports, and patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on maintaining documentation of past changes. However, in CIP-010-4 the core security objective of R1 was in Part 1.2 to authorize and document changes and the baseline configuration was used primarily to set the scope of those changes. Maintaining the baseline configuration information within 30 days after making changes is not a security objective, and as [Responsible Entities] implement more dynamic systems and more automation of change with virtualization, it becomes more problematic.
>
> In CIP-010-5, the [drafting team] considered the more dynamic, policy-based, and automated virtualization technologies … and determined to focus Requirement R1 on the true security objective of change management and authorizing intended changes for those changes that can affect the security posture. In other words, make R1.2 from version 4 the main focal point in version 5. Maintaining documentation of ever more automated updates to systems after the fact gives way in this version to authorizing changes that will affect the security posture of the system. The [drafting team] is addressing [Virtual Cyber Asset]s that may be dormant for long periods of time and dynamically patched at a future instantiation when needed. The [drafting team] considered the focus of R1 is not for entities to track the date/time a [Virtual Cyber Asset] may be dynamically instantiated and patched in an automated fashion in a remediation VLAN and then provide evidence that a baseline configuration was updated within 30 days of that dynamic event.
>
> In addition, with the introduction of application containers and orchestration (Kubernetes, Docker Swarm, etc.), application software may no longer be "installed" on a particular OS instance on a particular server. Instead, an orchestration service may instantiate an application container on the best "node" (server with container runtime) at the moment. For example, a dedicated "database server" gives way to a "database service" that can be instantiated in a container on any [Virtual Cyber Asset] or [Cyber Asset] managed by the orchestrator. Therefore, baseline configurations of statically installed software and open ports loses value as it becomes dynamically managed in these scenarios. The focus of R1 has thus

changed from documenting the installed software and its open ports on a Cyber Asset or [Virtual Cyber Asset] at some point post-change to authorizing the changes that will occur to it when it does instantiate, which provides more security value.

Entities may of course continue to maintain and use baseline configurations, but in CIP-010-5 it is no longer the singular prescribed way of setting change management scope and documenting changes. Baseline configurations may continue to be used as evidence for CIP-007 R1 for example, documenting the enabled ports on a system. In fact, baseline configurations will probably continue to be a very common method used by entities to help detect unauthorized changes in CIP-010 R2, but the standard does not prescribe it as the singular way to meet these security objectives. Therefore, the phrase "baseline configuration" has been removed from CIP-010-5 though entities may continue using it as their "how". Again, the focus of R1 in CIP-010-4 and CIP-010-5 is authorizing changes that affect the security posture of the applicable systems; the [drafting team] has just brough[t] it forward as the "what" with baseline configurations as one possible, but not prescribed, "how". Entities may also wish to reference [National Institute of Standards and Technology ("NIST")] SP 800-128 "Guide for Security-Focused Configuration Management of Information Systems" as a guide for additional information.

The [drafting team] also considered at length the scope of changes that should be subject to R1. In CIP-010-4, the scope was set by the prescribed elements in the baseline config, consisting essentially of software, patches, and ports. As mentioned above, the security objective of putting ports in the baseline configuration is not to document and maintain a list of listening ports; that security objective is covered in CIP-007 R1 to reduce the attack surface by disabling unneeded ports. Maintaining documentation of the patches installed on a system (which becomes more problematic over time with vendor-bundled monthly updates that may install/remove patches differently per each system's needs) is not the security objective. Knowing what patches are available and applicable to the systems and installing them and mitigating the risk is the goal as covered in CIP-007 R2. In CIP-010 R1, authorizing the action in order to manage change is the objective.

In addition, the [drafting team] considered the prescribed list of baseline configuration elements was insufficient as the scope of a change management requirement. For example, in a[] [Shared Cyber Infrastructure] that is configured to isolate [Virtual Cyber Asset]s of different impact levels from each other, managing and authorizing change to that configuration is vital. As Zero Trust architectures come to fruition, managing and authorizing changes to those access policies is crucial. These are all very important security configurations that were not enumerated in CIP-010-4's baseline configuration and thus not in scope. The [drafting team] concluded that creating a longer prescriptive list of items was not appropriate, in that such a list would need to be maintained as technology changes. The [drafting team] decided to put objective language in the requirement and use the Measures to show examples of more detailed lists of items.

…

The [drafting team] brought the security objective to the forefront in this requirement part by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the [drafting team] made conforming changes to Applicable Systems to add [Shared Cyber Infrastructure]. The [drafting team] considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping accomplished with the objective language of "…altered behaviors…" to the underlying technical controls so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories.

The [drafting team] used the objective language "…where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 and CIP-007, as defined by the Responsible Entity." The intent is to bound the scope to those changes that affect the system's CIP security posture. *More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements.*

The phrasing "alter the behavior of one or more cyber security controls" is intended to help clarify the scope. For example, the intent is that a user changing their password is not in scope; that is a change that may be required on some periodicity by a cyber security control such as a domain password policy but is not a change that alters the behavior *of the control itself*. What would be in scope is a change to that domain password policy.

The "excluding procedural and physical controls" (as well as the "*cyber security* controls" phrase) is intended to exclude from CIP-010 [Requirement] R1's scope changes to controls from CIP-005 and CIP-007 that are not technical controls. An example would be an entity may have signage or port-blockers as a procedural/physical control for meeting CIP-007 [Requirement R1 Part] 1.2 concerning physical ports. Installing/removing port blockers or changes to the signage is not intended to be subject to CIP-010 [Requirement] R1. A change to the affinity rules for a hypervisor, if the entity uses that in an [Shared Cyber Infrastructure] scenario to meet CIP-007 [Requirement] R1.3, would meet the intent, as well as changes to [Electronic Access Point] firewall rules/policy that the entity uses as the control to meet CIP-005 [Requirement] R1. The configuration of anti-malware controls the entity uses, such as update mechanisms or alerting mechanisms that change *how* the control functions in meeting CIP-007 [Requirement] R3 would be included but not the regular signature updates the control uses; those are not changes to the control's configuration that alter the way the control behaves.

Along these lines, rather than including a prescriptive list of change categories or types within the requirement, the [drafting team] did analyze the requirements in

> CIP-005 and CIP-007 and included examples of cyber security controls that may serve those requirements in the Measures column to help clarify the intent. These are examples and are not a mandatory prescriptive list of the types of changes that would be included and for which evidence of authorization through change records could be provided.
>
> It is important to note the [drafting team] did not include prescriptive timeframes for this requirement. The rationale for this is to account for emergency changes, those that need to occur for reliability of the system when it may not be possible to put in a request and gain authorization beforehand. The [drafting team] intent is for these system reliability related emergency changes to not become a violation of this standard, which it would if it had "prior to" type phrases within it, or required prescriptive definition of what constitutes emergency changes, etc. However, emergency changes will still need to be authorized, after the fact, to meet the requirement.[19]

As noted above, the shift to an objective-based approach within proposed CIP-010-5, Requirement R1 improves reliability of the BPS by focusing Responsible Entities on understanding how their security controls should be working and establishing forward-looking authorization for any changes that may impact how those controls work. Even for Responsible Entities implementing baseline configurations, such implementation under the objective-based requirement language will discourage Responsible Entities from treating the baseline as a documentation exercise only. To that end, Responsible Entities would need to understand which changes could impact the behavior of cyber security controls in CIP-005 and CIP-007. Such an approach is consistent with the principles underlying cyber security frameworks, such as NIST. For instance, controls within the configuration management family in NIST Special Publication 800-53 include those regarding configuration change control (CM-3) and impact analysis (CM-4) and support dynamic change control and monitoring, consistent with objectives in proposed CIP-010-5, Requirements R1 and R2. Similarly, the emphasis on behavior in proposed CIP-010-5 is

[19] Original Petition, Exhibit E-9 at pp. 5-6.

fully in line with the zero trust architecture tenet outlined in NIST Special Publication 800-27 that continuous validation of security control effectiveness is crucial to maintaining access and trust.

As with all proposed CIP Reliability Standards, regardless of how each Responsible Entity chooses to implement the revised requirements, the ERO Enterprise will assess through its CMEP activities whether Responsible Entities are implementing the proposed Reliability Standards in a manner that meets the requirement objective, is consistent with good cyber security practice, and is appropriate for each configuration.

D. Definitions and Phrases

As noted in the Original Petition, there are several proposed terms for addition to the Glossary of Terms Used in NERC Reliability Standards, and revisions include the replacement of the phrase "where technically feasible" with "per system capability." While the following subsections 1-3 provide excerpts from Exhibit E-12 to the Original Petition that highlight justification for some of the new terms, NERC reiterates that the definitions are not meant to stand alone but rather are used within the context of the Reliability Standards requirements. Each of the following terms were developed to define key components of virtualized environments: Shared Cyber Infrastructure, Virtual Cyber Asset, and Management Interface. In addition, subsection 4 below highlights additional detail on use of the phrase "per system capability." The excerpted information below would assist the Commission in further understanding the use of the new definitions and phrases.

1. Shared Cyber Infrastructure

The following excerpt from Exhibit E-12 to the Original Petition provides additional justification on the scope and use of shared resources within the Shared Cyber Infrastructure definition:

> The term [Shared Cyber Infrastructure] was defined to separate the underlying hardware from [Virtual Cyber Assets] in the situation where the shared hardware resources support [Virtual Cyber Assets] of varying impact levels. This allows security requirements to be targeted to [Shared Cyber Infrastructure] to address the unique risks of shared hardware. There are many requirements that now include the newly defined term [Shared Cyber Infrastructure] in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.
>
> Beyond security level parity with protecting a typical hardware based Cyber Asset, the [Shared Cyber Infrastructure] can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to [Shared Cyber Infrastructure], such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.
>
> The phrase "[Shared Cyber Infrastructure] does not include the supported [Virtual Cyber Assets] or Cyber Assets with which it shares its resources" is included to clarify that, for example, electronic access to a hosted [Virtual Cyber Asset] by a user is not electronic access to the [Shared Cyber Infrastructure] on which it executes.
>
> Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as [Shared Cyber Infrastructure]. However, network switches and other hardware that does enforce an [Electronic Security Perimeter], such as a network switch configured to host different VLANs to which systems of differing impact levels are connected, comes into scope as an [Electronic Access Control or Monitoring System].[20]

The use of the term Shared Cyber Infrastructure in the proposed Reliability Standards includes use in the Applicable Systems section of certain requirements. Therefore, the proposed new term helps ensure that appropriate cyber security protections are applied to a key component of a virtualized environment.

[20] Original Petition at Exhibit E-12, pp. 11-12.

2. Virtual Cyber Asset

The following excerpt from Exhibit E-12 to the Original Petition provides additional justification on the scope of the Virtual Cyber Asset, including information on application containers being considered software of a Virtual Cyber Asset or Cyber Asset:

> The term [Virtual Cyber Asset] was defined to allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined as is the case in the Cyber Asset definition. The NERC Glossary definition of Cyber Asset has a direct tie to its hardware and software ("including the hardware, software, and data in the device") and assumes the electronic device is self-contained with a one-to-one relationship between a device and its software (including the operating system). This affected the definitions of the "Applicable Systems" terms such as [BES Cyber System], [Electronic Access Control or Monitoring System], [Physical Access Control System], and [Protected Cyber Asset]s that were all based on the Cyber Asset definition. Because the Reliability Standard is applicable to the aforementioned systems, the security controls for the Cyber Assets also applies to the hardware. The one-to-one relationship between a Cyber Asset and its underlying hardware and software is what virtualization intentionally breaks to increase reliability and resiliency by allowing [Virtual Cyber Assets] to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.
>
> The phrase "currently executing on a virtual machine" is used to clarify:
>
> - That a [Virtual Cyber Asset] does not include disk image files that are not currently instantiated or executing and are thus providing no functions or services.
> - That a "logical instance of an operating system or firmware" only refers to those running on a hypervisor as a virtual machine and does not refer to a locally installed OS or firmware on the hardware.
>
> The definition excludes "logical instances that are being actively remediated…" to allow for automated solutions (such as remediation VLANs) to bring newly instantiated instances into

compliance in an isolated environment before they are moved to production networks and begin providing their function or service, at which point they become a [Virtual Cyber Asset].

The phrase "hosted on a BCA, EACMS, PACS, PCA, or SCI" is to clarify that an entity for an "all-in" scenario can still classify the underlying hardware as one or several of these types, yet the [Virtual Cyber Assets] remain their own object subject to requirements and are not simply "software in the device" as in the Cyber Asset definition.

Examples of [Virtual Cyber Assets] may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

The definition also clarifies that 'Application containers' (i.e., portable, packaged applications) are considered software of a [Virtual Cyber Asset] or Cyber Asset, though they may have some characteristics of a [Virtual Cyber Asset]. This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the [Virtual Cyber Asset] or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device.[21]

As detailed above, the proposed definition of Virtual Cyber Asset provides clarity around those virtualized assets that do not have a one-to-one relationship between software and hardware.

[21] Original Petition at Exhibit E-12, pp. 13-14

It also provides clarity on when certain behaviors of virtualized technologies are considered akin to a Cyber Asset within the CIP Reliability Standards. Therefore, the proposed term improves the reliability of the BPS through its use in ensuring that CIP Reliability Standards also account for the different relationship between hardware and software in a virtualized environment.

3. Management Interface

The following excerpt from Exhibit E-12 to the Original Petition provides background on the Management Interface definition, noting that the requirements within the Reliability Standards that use the definition inform its use and scope:

> The term Management Interface was defined so that requirements are established for [Shared Cyber Infrastructure] and [Electronic Access Control or Monitoring System] Management Interfaces to target the unique risks for virtualized environments presented by unrestricted access to the Management Interfaces for such environments. With 'infrastructure as a service' (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely access the console. It also includes interfaces used to configure an [Electronic Access Point] (such as on firewalls or a network switch that is enforcing an [Electronic Security Perimeter] between different virtual networks (e.g., VLANs). Note that scoping is included in requirements in the standard, not in the definition.[22]

Accordingly, in defining Management Interface, the proposed term improves the reliability of the BPS through ensuring that CIP Reliability Standards also account for the management plane in a virtualized environment. While the definition intentionally describes a management interface in a broad sense, the definition is further understood and scoped when used in the Reliability Standards. For instance, when used in proposed CIP-005-8, Requirement R1, Part 1.3, the

[22] Original Petition at Exhibit E-12, p. 11.

Management Interface is for the certain Shared Cyber Infrastructure and Electronic Access Control or Monitoring Systems creating the Electronic Security Perimeter, which could include, for example, the network switch that is configured with a VLAN and "controls" the Electronic Security Perimeter by defining what is and is not considered the Electronic Security Perimeter.[23] Therefore, the proposed definition is necessary to include such infrastructure within the CIP Reliability Standards requirements.

4. Technical Feasibility Exception

The Original Petition noted the declining trend in the use of Technical Feasibility Exceptions over the past several years.[24] As such, the drafting team replaced "where technically feasible" with the term "per system capability" to no longer trigger the use of the Technical Feasibility Exception process, which is administrative for both Responsible Entities and Regional Entities. Instead, the term "per system capability" is used in certain requirements. Should a Responsible Entity choose to rely on that term, the Responsible Entity will need to document the limit to the system's capability and demonstrate during compliance monitoring activities that the system's incapability prevents the Responsible Entity from implementing the control within the requirement.

E. COMPLIANCE MONITORING AND ENFORCEMENT

As noted in the Original Petition, the proposed Reliability Standards incorporate security objectives into requirements, and the Compliance Monitoring and Enforcement Program ("CMEP")[25] processes and procedures provide effective tools for monitoring and enforcing those

---

[23] Original Petition, Exhibit G, Document 370 at p. 118.
[24] Original Petition at pp. 28-30.
[25] NERC, *Rules of Procedure*, Section 400 et. seq.; Appendices 4B and 4C, https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC%20ROP%20effective%2020220825_with%20appendicies.pdf.

security objectives. NERC and the Regional Entities will use existing risk-based compliance monitoring processes to effectively monitor compliance with the new Reliability Standards requirements. As with any new Reliability Standard, NERC and the Regional Entities will provide training and collaborate on the security objectives to ensure that monitoring staff possess the necessary subject matter expertise to employ professional judgment in assessing compliance, consistent with applicable auditing principles.[26] In addition, NERC and the Regional Entities will likely use stakeholder engagement efforts, such as Small Group Advisory Sessions or entity assist visits, as appropriate, to help ensure both Responsible Entities and monitoring staff are prepared for implementation. The ERO Enterprise will also consider using CMEP Practice Guides under the NERC Compliance Guidance Policy, as appropriate, to help ensure consistency across Regional Entities' monitoring or enforcement practices. Any potential CMEP Practice Guide would incorporate lessons learned from the Small Group Advisory Sessions. Along those lines, the drafting team in its response to comments in the record of the Original Petition also recommended that pre-qualified organizations under the NERC Compliance Guidance Policy consider issuing any Implementation Guidance to help guide Responsible Entities' compliance approaches in meeting the security objectives.

Should a Potential Noncompliance[27] go through enforcement processes for disposition, the existing enforcement processes provide effective means for assessing such findings in a fair and non-preferential manner. For each finding assessed, NERC and the Regional Entities consider the facts and circumstances surrounding each violation and use professional judgment to assess

[26] United States Government Accountability Office, *Government Auditing Standards*, Requirement 3.109 (2024), https://www.gao.gov/assets/d24106786.pdf.

[27] *See N. Am. Elec. Reliability Corp. Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure* (effective May 19, 2022) at 17 ("Potential Noncompliance" means the identification, by the Compliance Enforcement Authority, of a possible failure by a Registered Entity to comply with a Reliability Standard that is applicable to the Registered Entity), https://www.nerc.com/AboutNERC/RulesOfProcedure/ROP_Appendix%202_20220519.pdf.)

whether security objectives were met, consistent with the FERC-approved Sanction Guidelines.[28] This ensures that enforcement actions bear a reasonable relationship to the seriousness of the violation.[29] In applying such guidelines to requirements with security objectives, NERC and the Regional Entities can follow a repeatable process while ensuring each Responsible Entity is treated fairly based on the unique facts and circumstances of each Potential Noncompliance.

[28] *See Sanction Guidelines of the North American Electric Reliability Corporation* (effective January 19, 2021) at 3, https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_4B_effective%2020210119.pdf .
[29] *Id.*

IV. CONCLUSION

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

- the proposed Reliability Standards in the Original Petition, and as amended herein;
- the proposed Implementation Plan as proposed in the Original Petition; and
- the retirement of Reliability Standards effective as proposed in the Original Petition.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Assistant General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
Marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: May 20, 2025

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 1

CIP-003-10
(Redline)

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10~~9~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against 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-003-~~9~~10:

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

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

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. 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.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for CIP-003-9.~~."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP-~~-~~004);

1.1.2. Electronic Security Perimeters (CIP-~~-~~005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP-~~-~~006);

1.1.4. System security management (CIP-~~-~~007);

1.1.5. Incident reporting and response planning (CIP-~~-~~008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP-~~-~~009);

1.1.7. Configuration change management and vulnerability assessments (CIP-~~-~~010);

1.1.8. Information protection (CIP-~~-~~011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-~~-~~002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-~~-~~002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that

supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods 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 (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.1)	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (Part ~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS~~BES Cyber Systems~~, but did not address one of the seven topics required by Requirement R1. (Part~~R~~1.2) OR	cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address two of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16	cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address three of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required	previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by ~~R1~~Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but~~ did not address four or more of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not have any documented cyber

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~BES Cyber Systems~~ as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part ~~R~~1.2)	by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part~~R~~1.2)	security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	equal to 16 calendar months of the previous approval. (~~R1~~Part 1.2)			
R2	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~ according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for~~	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity ~~that provides access to low impact BES Cyber System(s), per Cyber Asset capability~~ according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES~~	The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Transient Cyber Assets and Removable Media, but~~ failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	~~Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)		
R3	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identif~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-003-5.	
6	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.

Version	Date	Action	Change Tracking
6	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.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple~~-~~-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s~~),~~) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP~~-~~-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~between~~Between:

- a low impact ~~BES Cyber System(s)~~ BCS; or
- An SCI that supports a low impact BCS

and a Cyber ~~Asset~~System(s) outside the asset containing ~~low impact BES Cyber System(s);~~:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

~~i.~~ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s);~~BCS or SCI that supports a low impact BCS; and

~~ii.~~iii. not used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices (e.g.,~~ communications ~~using protocol IEC TR-61850-90-5 R-GOOSE).~~of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s),~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For ~~Transient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per ~~Transient Cyber Asset~~TCA 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.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset~~(per TCA 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~~Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset.~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e~~-~~-mails, memos, or computer~~-~~-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets ~~containing low impact BES Cyber Systems,~~ , the routable protocol communication ~~between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset~~as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that ~~communication is~~communications are used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices~~communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 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~~TCA 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~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 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 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)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA 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~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on~~-~~-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, 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 the 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~~.~~

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
    - other operational, procedural, or technical controls.
3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 2-A

CIP-006-7.1
(Clean)

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7.1

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) 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 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-006-7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 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.

4.3. "Applicable Systems**":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific Requirement Part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7.1 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7.1 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP .
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7.1 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7.1 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7.1 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7.1 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7.1 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7.1 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7.1 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods 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 Assessment Processes:** 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 (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-006-7 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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees	Virtualization Modifications
7.1	4/16/25	Approved by the Standards Committee	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 2-B

CIP-006-7.1
(Redline)

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-~~6~~7.1

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) 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 ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ 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 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 ~~SPS or~~ RAS where the ~~SPS or~~ 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-006-~~6~~7.1:

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

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

~~**4.2.3.2**~~**4.2.3.3** Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3**~~**4.2.3.4** 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**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5**~~**4.2.3.6** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

~~**5. Effective Dates:**~~

~~See Implementation Plan for CIP-006-6.~~

~~**6. Background:**~~

~~Standard CIP-006 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:~~

4.3. <u>":</u> Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific ~~requirement row~~<u>Requirement Part</u> 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 "Applicable Systems" 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.~~

- ~~**Medium Impact BES Cyber Systems without External Routable Connectivity –** Only applies to medium impact BES Cyber Systems without External Routable 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.~~
- ~~**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.~~
- ~~**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.~~

5. ~~**Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

   Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium ~~I~~impact ~~BES cyber Systems~~ BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High ~~I~~impact ~~BES Cyber Systems~~BCS, or • Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	~~An example~~Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium ~~i~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An example~~Examples of evidence may include, but are not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA ~~-~~SCI supporting an Applicable System in this Part	~~Where technically feasible, utilize~~Utilize two or more different physical access controls (this does not require two completely independent ~~physical access control systems~~PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSPs to only those individuals who have authorized unescorted physical access~~.~~ , per system capability.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in the physical security plan that describes ~~the Physical Security Perimeters~~each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.	Examples ~~An example~~ of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.
1.5	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~ PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High i~~I~~mpact ~~BES Cyber Systems~~ BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Monitor each ~~Physical Access Control System~~ PACS for unauthorized physical access to a ~~Physical Access Control System~~ PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	~~Physical Access Control Systems~~ (PACS~~)~~ associated with: • High i~~I~~mpact ~~BES Cyber Systems~~BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~ PACS to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of the detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to ~~Physical Access Control Systems~~ PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA ~~-~~Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP ~~Physical Security Perimeter~~ and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the individual and the date and time of entry into each PSP ~~Physical Security Perimeter~~.
1.9	High i~~I~~mpact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact BCS ~~BES Cyber Systems~~ with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP ~~Physical Security Perimeter~~ for at least 90 calendar days.	Examples ~~An example~~ of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the date and time of entry into each PSP~~Physical Security Perimeter~~.

CIP-006-~~6~~7.1 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ ~~• encryption of data that transits such cabling and components; or~~ ~~• monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ ~~• an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7.1 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter, except during CIP Exceptional Circumstances.~~PSP.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Physical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High ~~i~~Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium ~~i~~Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from each ~~Physical Security Perimeter~~ PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	Examples ~~An example~~ of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeter~~ PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

	SCI supporting an Applicable System in this Part		

CIP-006-~~6~~7.1 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7.1 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7.1 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC Locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at ~~the Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

~~1.1.~~ Compliance Enforcement Authority:

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~1.3.~~ Evidence Retention:

1.2. The following evidence retention periods 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.

~~1.4.~~ Compliance Monitoring and Assessment Processes:

~~1.5.~~1.3. As defined in the NERC Rules of Procedure, "Compliance ~~Audits~~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.

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.6. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter. (~~PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems. (~~PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each ~~Physical Security Perimeter~~PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical~~

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter. (~~PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required

R #	Violation Severity Levels (CIP-006-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

- Implementation Plan for Project 2016-02
- CIP-006-7 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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	~~TBD~~5/9/24	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees	Virtualization Modifications
7.1	4/16/25	Approved by the Standards Committee	Errata

~~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.~~

~~General:~~

~~While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.~~

~~Requirement R1:~~

~~Methods of physical access control include:~~

- ~~Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~
- ~~Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~
- ~~Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~

- ~~Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.~~

~~Methods to monitor physical access include:~~

- ~~Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~
- ~~Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.~~

~~Methods to log physical access include:~~

- ~~Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.~~
- ~~Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~
- ~~Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.~~

~~The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single-perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.~~

~~Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the~~

~~physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.~~

~~This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.~~

~~The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.~~

~~The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.~~

~~The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be~~

~~implemented on third-party components when entities rely on leased third-party communications.~~

~~In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.~~

~~Requirement R2:~~

~~The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.~~

~~The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.~~

~~Requirement R3:~~

~~This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.~~

~~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:~~

~~Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable~~

~~communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.~~

~~Rationale for Requirement R2:~~

~~To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~Rationale for Requirement R3:~~

~~To ensure all Physical Access Control Systems and devices continue to function properly.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 3-A

CIP-007-7.1
(Clean)

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7.1

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against 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 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-007-7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 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.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See Project 2016-02 Modifications to CIP Standards Implementation Plan.

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-007-7.1 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

CIP-007-7.1 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R2 – Cyber Security Patch Management*. *[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-007-7.1 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.
2.3	High impact BES Cyber Systems and their	For applicable patches identified in Part	Examples of evidence may include, but

CIP-007-7.1 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High impact BCS and their associated:	For those methods identified in Part 3.1	Examples of evidence may include, but

CIP-007-7.1 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7.1 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. Compliance Enforcement Authority:
   As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention:
   The following evidence retention periods 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 Assessment Processes:
   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.

   1.4. Additional Compliance Information:
   None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7.1 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-7.1 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-007-5.	
6	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.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses

Version	Date	Action	Change Tracking
			remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	TBD	Approved by the Standards Committee	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 3-B

CIP-007-7.1
(Redline)

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-~~6~~7.1

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against 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 ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ 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 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 ~~SPS or~~ RAS where the ~~SPS or~~ 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-007-~~6~~7.1:

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

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

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 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~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-007-6.~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires 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:~~

~~5.1.~~4.3. ~~":~~ Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part 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 "Applicable Systems" 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.~~

- ~~**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 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.~~
- ~~**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 in the applicability column. 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.~~

5. ~~**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.~~**Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

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-007-~~6~~7.1 Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R1 – ~~Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7.1 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control~~Medium Impact BES Cyber~~ Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~on all applicable Cyber Assets and Electronic Access Points, individually~~ or ~~by group.~~network accessible logical services, individually or by group; • Listings of the listening ports ~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; ~~or~~ • Configuration ~~files~~or settings of

CIP-007-~~6~~7.1 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part.		host-based firewalls or other device level mechanisms that ~~only allow~~disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed ~~ports and deny all others.~~ network accessibility.

CIP-007-~~6~~7.1 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~i~~impact ~~BES Cyber Systems~~BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~i~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R2 – Cyber Security Patch Management*. *[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-007-~~6~~7.1 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7.1 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches ~~for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis.~~ .
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS;	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security ~~related~~ patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~7.1 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
2.3	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; ~~or~~ • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System Component~~component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

CIP-007-~~6~~7.1 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7.1 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated:	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-~~6~~7.1 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
3.3	High ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7.1 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events ~~at the BES Cyber System level (~~, per ~~BES Cyber System~~system capability~~) or at the Cyber Asset level (per Cyber Asset capability)~~, for identification of, and after-the-fact investigations of, Cyber Security Incidents that ~~includes, as~~include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber~~Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~l~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated:	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events ~~(~~, per ~~Cyber Asset or BES Cyber System~~system capability~~):~~: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~7.1 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
4.3	High ~~i~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~i~~impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, retain~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~i~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7.1 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use ~~for the BES Cyber System~~.
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems~~Cyber Asset~~; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System~~Cyber Asset~~.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~7.1 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or ~~G~~generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods 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 Assessment Processes:

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

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.

1.4. Additional Compliance Information:

None

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~R1~~The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7.1 Table R1. (Requirement R1)	The Responsible Entity ~~has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity ~~did not implement or document~~neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-7.1~~6~~ Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security~~	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes,	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~7.1 Table R2. (Requirement R2)

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~patches for applicability but~~ did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	including the identification of sources, for tracking or evaluating cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable	installing cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the	OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	evaluation completion. (Part 2.3)	
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but,~~ where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7.1 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling~~ of ~~logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify~~	the applicable items in CIP-007-~~6~~ 7.1 Table R4. (Requirement R4) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (~~, per ~~device or~~ system capability~~) but~~, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7.1 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for~~	~~System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the~~The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more~~

R #	Violation Severity Levels (CIP-007-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	~~documented process(es) for password only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~neither limited the number of unsuccessful authentication attempts ~~or generate~~nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 Technical Rationale

~~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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-007-5.	
6	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.
6	2/15/15	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

Version	Date	Action	Change Tracking
			No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	~~TBD~~5/9/24	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees	Virtualization Modifications
7.1	4/16/25	Approved by the Standards Committee	Errata

~~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:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~1.1.~~ ~~This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~

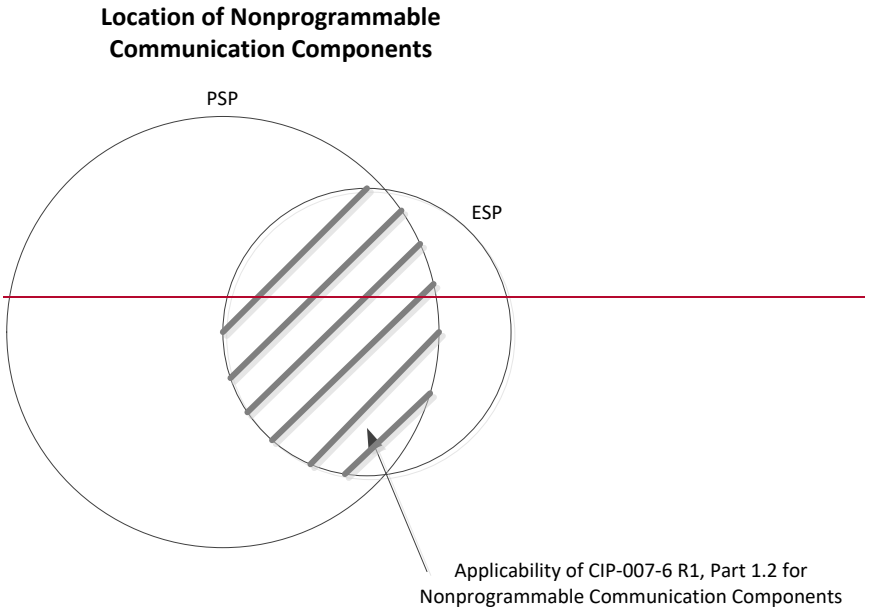
~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~

~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense in depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~



~~Requirement R2:~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

~~Detected known or potential malware or malicious activity~~

~~Failure of security event logging mechanisms~~

~~Login failures for critical accounts~~

~~Interactive login of system accounts~~

~~Enabling of accounts~~

~~Newly provisioned accounts~~

~~System administration or change tasks by an unauthorized user~~

~~Authentication attempts on certain accounts during non-business hours~~

~~Unauthorized configuration changes~~

~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~**Requirement R5:**~~

~~Account types referenced in this guidance typically include:~~

~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~

~~Individual user account: An account used by a single user.~~

~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~

~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~

~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~

~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~

~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~

~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or~~

~~installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~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 requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 4-A

CIP-008-7.1
(Clean)

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7.1

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

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 Bulk Electric System (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 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-008-7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 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.

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

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

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. Compliance Enforcement Authority:
   The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

   1.2. Evidence Retention:
   The following evidence retention periods 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 Assessment Processes:
   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 (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column. (Requirement R4)	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 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		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
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-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Version	Date	Action	Change Tracking
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	TBD	Approved by the Standards Committee	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 4-B

CIP-008-7.1
(Redline)

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~6~~7.1

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

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:~~Bulk Electric System (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 ~~Remedial Action Scheme~~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 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 ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~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-008-~~6~~7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

~~**4.2.3.3**~~**4.2.3.4** 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**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5**~~**4.2.3.6** Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. ~~**5. Effective Dates:**~~

~~See Implementation Plan for CIP-008-6.~~

~~**6. Background:**~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 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 must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it 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 particular 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 rowpart 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 "Applicable 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.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-~~6~~7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated~~:~~ Electronic Access Control or Monitoring Systems (EACMS) Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the ~~"~~Applicable Systems~~"~~ column for this Part; and	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column including justification for attempt determination criteria and documented processes for notification.

CIP-008-~~6~~7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.2.3 To provide notification per Requirement R4.	
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-~~6~~7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every~~-~~ 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-~~6~~7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-~~6~~7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-~~6~~7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of~~-~~ post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or ~~•~~ Training sign-in sheets. •

~~CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication~~			
~~**Part**~~	~~**Applicable Systems**~~	~~**Requirements**~~	~~**Measures**~~
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	~~An example~~Examples of evidence may include, but ~~is~~are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-~~6~~7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States ~~National~~ Cybersecurity ~~and Communications Integration Center (NCCIC),~~[1] & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-~~6~~7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column according to the applicable requirement parts in *CIP-008-~~6~~7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-~~6~~7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.

[1] ~~The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-~~6~~7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	• One hour after the determination of a Reportable Cyber Security Incident. • ~~By~~ the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part. •	
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within ~~7~~seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC.~~CISA, or their successors.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
The following evidence retention periods 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 Assessment Processes:

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~**2. Table of Compliance Elements**~~

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 (CIP-008-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but the plan does~~Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but the plan does~~Entity's plan did	The Responsible Entity ~~has~~did not ~~developed~~develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible ~~Entity has developed a Cyber Security Incident response~~Entity's plan~~, but the plan does~~ did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column for Part 1.2. (Part 1.2)

R #	Violation Severity Levels (CIP-008-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	
R2	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for Part 2.2 occurs. (Part 2.2)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for Part 2.3. (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or	The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2)	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity ~~notified E-ISAC and NCCIC, or their~~	The Responsible Entity ~~failed to~~did not notify E-ISAC or	The Responsible Entity ~~notified E-ISAC and NCCIC, or their~~	The Responsible Entity ~~failed to~~did not notify E-ISAC and

R #	Violation Severity Levels (CIP-008-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR ~~The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to~~The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable~~	~~NCCIC~~CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column. (Requirement R4)	~~successors, of a Reportable Cyber Security Incident but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to~~did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

~~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		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
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-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

7	~~TBD~~5/9/24	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	TBD	Approved by the Standards Committee	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 5-A

CIP-009-7.1
(Clean)

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7.1

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of 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 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-009-7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems

providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7.1 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7.1 Table R1 – Recovery Plan Specifications*.

CIP-009-7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.
1.4	High impact BCS and their associated:	One or more processes to verify the	Examples of evidence may include, but are

CIP-009-7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	successful completion of the backup processes in Part 1.3 and to address any backup failures.	not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g., sample tape load, browsing tape contents) and compatibility with current system configurations (e.g., manual, or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to:

CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
		defined role in the recovery plan of the updates.	• Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods 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 Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 15 calendar months, not exceeding 16	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2)	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar months, not exceeding 18	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan(s)

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications

Version	Date	Action	Change Tracking
7.1	TBD	Adopted by the NERC Standards Committee.	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 5-B

CIP-009-7.1
(Redline)

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-~~6~~7.1

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of 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 ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~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 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 Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme~~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-009-~~6~~7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 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~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-009-6.~~

~~6. Background:~~

~~Standard CIP-009 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 their documented processes, but they 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:~~

~~5.1.~~4.3. ~~":~~ Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part 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 "Applicable Systems" 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.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and 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 include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

- ~~**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.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7.1 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7.1 Table R1 – Recovery Plan Specifications*.

CIP-009-~~6~~7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-~~6~~7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.
1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples ~~An example~~ of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system ~~Cyber Asset~~ capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples ~~An example~~ of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7.1 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7.1 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~6~~7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and ~~2.~~ PACS ~~3.~~2.	Test a representative sample of information used to recover ~~BES Cyber~~Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, operational logs or test results with criteria for testing the usability (e.g~~.~~., sample tape load, browsing tape contents) and compatibility with current system configurations (e.g~~.~~., manual, or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-~~6~~7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7.1 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the ~~applicable requirement~~Applicable Requirement parts in *CIP-009-~~6~~7.1 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~6~~7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~-~~the ability to execute the recovery plan:	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or

CIP-009-~~6~~7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods 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 Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible ~~Entity has developed recovery~~Entity's plan(s~~), but the plan(s) do~~) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery~~ plan(s~~), but the plan(s) do~~) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has~~did not ~~created~~create recovery plan(s) for ~~BES Cyber~~Applicable Systems. OR The Responsible Entity ~~has created recovery~~ plan(s) ~~for BES Cyber Systems, but the plan(s) does~~did not address the conditions for activation in Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the plan(s) does~~plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR

R #	Violation Severity Levels (CIP-009-6~~7~~.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests of the plan~~.~~ ~~(~~(s). (Part 2.1) OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan~~.~~ ~~(~~(s). (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar	The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days ~~-~~of each	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan

R #	Violation Severity Levels (CIP-009-~~6~~7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the update being completed. (Part 3.1.3)	plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or ~~–~~responsibilities, or • Responders, or • Technology changes. (Part 3.2)	recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	test or actual recovery. (Part 3.1.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

~~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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
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-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	~~TBD~~5/9/24	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees.	Virtualization Modifications

Version	Date	Action	Change Tracking
7.1	4/16/25	Approved by the Standards Committee	Errata

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:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

~~A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.~~

~~For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.~~

~~For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.~~

~~For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:~~

1. ~~Installation files and media;~~
2. ~~Current backup tapes and any additional documented configuration settings;~~
3. ~~Documented build or restoration procedures; and~~
4. ~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

- ~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~
- ~~Non-periodic backup process – If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~
- ~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~
- ~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

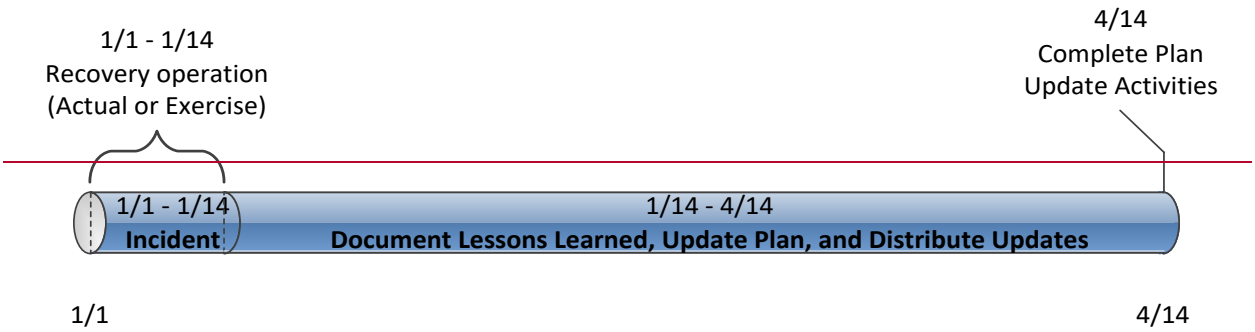


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

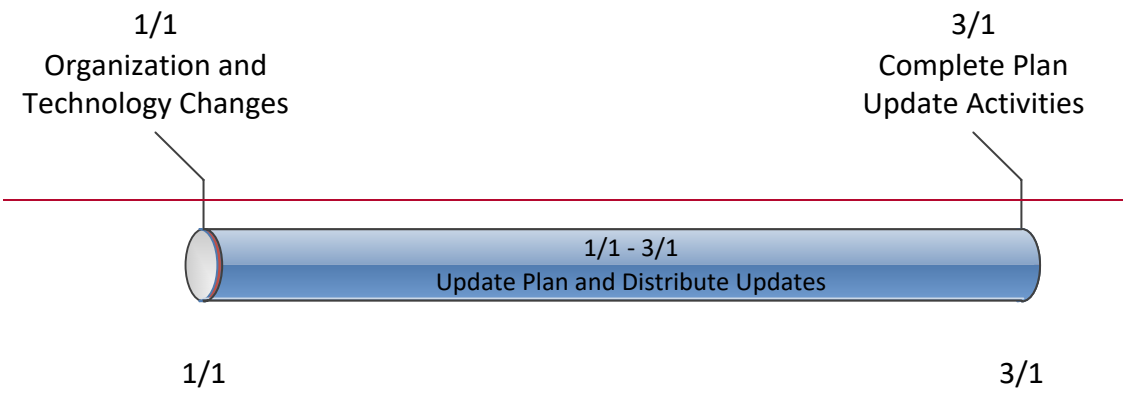


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

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:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 6-A

CIP-011-4.1
(Clean)

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4.1

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against 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 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-011-4.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 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.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4.1 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4.1 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4.1 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include

CIP-011-4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4.1 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-4.1 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4.1 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. 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:

- The 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 (CIP-011-4.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4.1 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
4.1	TBD	Adopted by the Standards Committee	Errata

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit 6-B

CIP-011-4.1
(Redline)

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-~~3~~4.1

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against 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 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-011-34.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3**~~**4.2.3.4** 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~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

~~1. **Effective Dates:** See Implementation Plan for CIP-011-3.~~

~~2. **Background:** Standard CIP-011 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:

4.3. ": Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement rowpart 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

- B. **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.

Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~"~~Applicable Systems~~"~~ identified in *CIP-011-~~3~~4.1 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-~~3~~4.1 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~3~~4.1 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High ~~i~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~i~~impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include

CIP-011-~~3~~4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-34.1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-34.1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-34.1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systemsimpact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systemsimpact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Prior to the release forMethods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.).	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-34.1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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 3.1.PCA	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. 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:

- The 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 (CIP-011-~~3~~4.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). ~~(~~ (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include processes for reuse to prevent the unauthorized retrieval of BCSI from ~~the BES Cyber Asset~~an Applicable System. (Part 2.1)	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System~~the BES Cyber Asset~~. (Part 2.1)	The Responsible Entity ~~has not~~neither documented ~~or~~ nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD5/9/24	Virtualization ModificationsAdopted by NERC Board of Trustees.	Virtualization Modifications
4.1	TBD	Adopted by the Standards Committee	Errata