NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda
Standards Committee Conference Call

January 20, 2021 | 1:00—3:00 p.m. Eastern

Dial-in: 1-415-655-0002 | Access Code: 180 585 7645 | Meeting Password: 012021
Click here for: WebEx Access

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement*
NERC Participant Conduct Policy

Agenda Items

1. **Review January 20 Agenda - Approve - *Amy Casuscelli*** (1 minute)
2. **Consent Agenda - *Amy Casuscelli*** (5 minutes)
   a. December 9, 2020 Standards Committee Meeting Minutes* - **Approve**
3. **Projects Under Development - Review**
   a. Project Tracking Spreadsheet - *Charles Yeung* (5 minutes)
   b. Projected Posting Schedule - *Howard Gugel* (5 minutes)
4. **Standards Committee Executive Committee* – Elect – *Amy Casuscelli***
5. **Project 2019-06 Cold Weather* - Authorize - *Soo Jin Kim*** (15 minutes)
   a. 2019-06 Implementation Plan*
   b. 2019-06 IRO-010-4*
   c. 2019-06 TOP-003-5*
   d. 2019-06 EOP-011-2*
6. **Project 2016-02 Modifications to CIP Standards *- Authorize - *Soo Jin Kim*** (15 minutes)
   a. 2016-02 Definitions*
   b. 2016-02 Implementation Plan*
   c. 2016-02 CIP-002-7*
   d. 2016-02 CIP-003-9*
   e. 2016-02 CIP-004-7*
   f. 2016-02 CIP-005-8*

   g. 2016-02 CIP-006-7*

   h. 2016-02 CIP-007-7*

   i. 2016-02 CIP-008-7*

   j. 2016-02 CIP-009-7*

   k. 2016-02 CIP-010-5*

   l. 2016-02 CIP-011-3*

   m. 2016-02 CIP-013-3*

7. **Standard Authorization Request for IRO-010-2 and TOP-003-3* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. IRO-010-2 and TOP-003-3 Standard Authorization Request*

8. **Standard Authorization Request for MOD-025-2* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. MOD-025-2 Standard Authorization Request*

9. **Standard Authorization Request for PRC-019-2* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. PRC-019-2 Standard Authorization Request*

10. **Standard Authorization Request for PRC-023-4* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. PRC-023-4 Standard Authorization Request*

11. **Standard Authorization Request for PRC-002-2* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. PRC -002-2 Standard Authorization Request*

12. **Standard Authorization Request for VAR-002-4.1* – Accept/Authorize/Authorize - *Soo Jin Kim*** (15 minutes)

   a. VAR-002-4.1 Standard Authorization Request*

13. **Legal Update and Upcoming Standards Filings* - Review – *Marisa Hecht*** (5 minutes)

14. **Informational Items - Enclosed**

   a. Standards Committee Expectations*

   b. 2021 SC Meeting Schedule

   c. 2021 Standards Committee Roster

   d. Highlights of Parliamentary Procedure*

15. **Adjournment**

*Background materials included.

Public Meeting Notice

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

Conference call/webinar version:

As a reminder to all participants, this webinar is public. The registration information was posted on the NERC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Face-to-face meeting version:

As a reminder to all participants, this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

For face-to-face meeting, with dial-in capability:

As a reminder to all participants, this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Minutes
Standards Committee Conference Call

December 9, 2020 | 1:00–3:00 p.m. Eastern

A. Casuscelli, chair, called to order the meeting of the Standards Committee (SC or the Committee) on December 9, at 1:00 p.m. Eastern. C. Larson, secretary, called roll and determined the meeting had a quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement

The Committee secretary called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice and directed questions to NERC's General Counsel, Sonia C. Mendonça.

Introduction and Chair's Remarks

A. Casuscelli welcomed the Committee and guests, and acknowledged the people attending as proxies.

Review December 9, 2020 Agenda (agenda item 1)

The Committee approved the December 9, 2020 meeting agenda.

Consent Agenda (agenda item 2)

The Committee approved the November 19, 2020 SC meeting minutes by unanimous consent. The Committee approved the 2021-2023 Standards Committee Strategic Work Plan and 2020 Standard Committee Accomplishments by unanimous consent.

Projects Under Development (agenda item 3)

C. Yeung reviewed the Project Tracking Spreadsheet. S. Kim delivered an overview of the three month outlook. N. Shockey questioned if there is a better way to track and log incoming SARs, and whether this is appropriate for PMOS to track. S. Kim and H. Gugel shared that NERC staff, SC and PMOS leadership will consider options to provide more transparency of incoming SARs. H. Gugel reviewed the Projected Posting Schedule.

Project 2020-01 Modifications to MOD-032-1 (agenda item 4)

S. Kim provided an overview of the SAR drafting team recommendation. M. Hostler motioned to reject the SAR, since he felt the concerns raised by industry in opposition of the SAR were not addressed. H. Gugel shared that the SAR had been previously endorsed by the Planning Committee and the Standards Committee had accepted and authorized for informal posting of the SAR during the March meeting. C. Larson, developer on the project, noted that the SAR was posted for an informal comment period, and the SAR Drafting Team did provide a response to comments. The SAR Drafting Team felt the SAR was worded broadly enough to allow due consideration of industry comment during the standard development process. The Committee members discussed the merits of industry comments and the SAR Drafting Team response to comments and if the SAR should be accepted or rejected.

M. Hostler moved to reject the Standards Authorization Request (SAR) revised by the Project 2020-01 Modifications to MOD-032-1 SAR Drafting Team, and provide a written explanation for rejection to the submitter within 10 days.

The Committee approved the motion with Sean Bodkin, Linn Oelker, Kent Feliks, Barry Lawson, Marty Hostler, Bill Winters, Rebecca Darrah, Sarah Snow, David Kiguel, and Robert Blohm supported. Michael Puscas, John Babik, Charles Yeung, Donova Crane (proxy for Steve Rueckert), and Tony Purgar opposed. Neil Shockey, Venona Greaff, and Ajinkya Rohanker abstained.

The Committee approved the motion.

Project 2020-04 Modifications to CIP-012 (agenda item 5)
S. Kim provided an overview of the SAR drafting team recommendation.

S. Bodkin moved to accept the Standards Authorization Request (SAR) revised by the Project 2020-04 Modifications to CIP-012-1 SAR Drafting Team, appoint the current SAR drafting team as the Project 2020-02 Modifications to CIP-012-1 Standard Drafting Team (SDT), and authorize drafting as proposed in the SAR.

The Committee approved the motion with no objections. Marty Hostler abstained.

Standards Efficiency Review Recommendations (agenda item 6)
M. Puscas provided an overview of the project recommendations.

S. Bodkin made a motion to endorse the recommendation for the Standards Committee Process Subcommittee (SCPS) in coordination with NERC staff to review the Reliability Standards Template, Drafting Team Training Modules, and Drafting Team Reference Manual.

The Committee approved the motion with no objections or abstentions.

PMOS Scope (agenda item 7)
C. Yeung provided a background of the changes made to the PMOS Scope document. Committee members discussed the language around the subject of preregistration for meetings. S. Bodkin expressed a concern that the additional language could be used to block someone from attending a meeting. It was noted that this language is also in the SC charter and is needed during for those who host in-person meetings as they might need individuals attending to preregister for security issues. A new version of the PMOS Scope document will be posted on NERC website.

V. Greaff moved to approve the revised version of the PMOS Scope document as written.

The Committee approved the motion with no abstentions. S. Bodkin opposed.

SC Orientation (agenda item 8)

A. Casuscelli shared an overview of the SC member orientation reference document. This document formalizes the new SC members onboarding and will be used for the first time with the new members beginning their terms in 2021.

SCEC Nominations (agenda item 9)
C. Larson provided a reminder to the SC for those interested in being on the SC Executive Committee (SCEC) to submit their nominations, appointments will occur at the January 2021 SC Meeting.

Legal Update and Upcoming Standards Filings (agenda item 10)
M. Hecht provided the legal update regarding recent and upcoming filings.

Adjournment
A. Casuscelli thanked committee members and observers and adjourned the meeting at 2:48 p.m. Eastern.

Agenda Item 4
Standards Committee
January 20, 2021

2021 Standards Committee Executive Committee Nominations

Action

Elect representatives to the Standards Committee Executive Committee.

Background

In accordance with the Standards Committee Charter, the Standards Committee Executive Committee shall have an Executive Committee (SCEC) consisting of five members, including the Committee officers plus three segment members, elected by the Committee. The three segment members cannot represent the same industry segments the Committee officers previously represented, nor can any two of the segment members be from the same segment. The Executive Committee will be elected annually at the January Committee meeting. The Executive Committee shall meet when necessary between regularly-scheduled Committee meetings to conduct Committee business.

Current SC officers include:

- SC Chair: Amy Casuscelli, Xcel Energy, Formerly representing Segment 5
- SC Vice Chair: Todd Bennett, AECI, Formerly representing Segment 3

Nominations

NERC staff received nominations from three Standards Committee members to serve on the Standards Committee Executive Committee:

Michael Puscas, Independent System Operator of New England (ISO-NE), Segment 2

Dr. Michael Puscas is a Compliance Manager for the Independent System Operator of New England (ISO-NE) managing compliance with the Operation and Planning (O&P) set of NERC Standards. He's been involved in NERC compliance-related issues and management for over 20 years. He was a Director of Compliance at AvanGrid (formerly United Illuminating), Senior Manager of CIP Compliance for Eversource (formerly Northeast Utility). He works closely with the ISO RTO Council (IRC) and more specifically the IRC's Standards Review Committee (SRC) assessing and evaluating real or proposed changes to NERC Standards and evaluating the impact on the organization. Michael is also a contributing member and former Vice-Chair of the Compliance Working Group (CWG) reporting to the SRC.

Michael is well versed in compliance risks and internal controls as a result of leading the effort for ISO-NE and providing guidance and leadership in these areas for other companies through heavy participation in multiple committees. He is a voting member of Segment 2 and works closely with NERC's Standards Committee (SC). In addition, he provides guidance and leadership for the North American Transmission Forum (NATF). Michael is currently the Chair of the Risk, Controls and Compliance (RCC) committee for NATF where he leads a nation-wide committee to discuss compliance-related subjects and emerging issues. Michael works with other team members on NERC's Standard Efficiency Review (SER) team for both Phase 1 and Phase 2. His work on this committee continues. He is the primary compliance contact for NPCC and is an alternate member of NPCC's Compliance Committee (CC).

In addition, Michael was the Y2K Project Manager for the Millstone Nuclear Power Plant, Waterford, CT assuring all software systems were fully Y2K compliant. He led the Internal Control Evaluation (ICE) effort for ISO-NE in 2018, and is currently leading the effort for the same evaluation in 2020. He has designed internal control models and created new internal control tracking, testing, and designed, developed and implemented a new Compliance Management Database for ISO-NE.

Michael is adept at working in a collaborative team environment to develop comments and recommendations related to new and modified NERC Standards. Michael is highly organized, analytical, perceptive, hard-working, and intelligent. He brings a wealth of compliance and electrical industry experience in operations, planning, and cyber systems security. He has designed, developed and implemented new and innovative compliance tools and key performance metrics (KPIs) and helped compliance organizations grow and mature. He possesses a balanced mix of both compliance and technical skills.

Barry Lawson, National Rural Electric Cooperative Association, Segment 4
Please accept my expression of interest in being reelected to the SCEC. I've been a member of the SC for the TDU segment for five years, and prior to that, I've participated in SC meetings and discussion for several years. I have a deep understanding of the SPM and a broad range of NERC policy and governance issues. Over the last 11 years I've been a member of two drafting teams focusing on Back-Up Control Centers and the BES Definition. I was the Vice Chair of the BES Definition drafting team. With this experience and background relevant to the SC, I would be pleased to again be considered for the SCEC. Briefly, for additional background, my career has provided me with excellent opportunities at NRECA, KEMA Consulting, Columbia Natural Gas Transmission, EEI and Dominion Energy.

Venona Greaff, Occidental Chemical Corporation, Segment 7
Venona is the team lead for Occidental's NERC compliance program. She is responsible for working directly with Oxy's NERC Registered Entities to ensure compliance with Reliability and CIP Standards applicable to Occidental's Registered Entities. She leads the implementation and communication of Oxy's Internal Compliance Program. Her leadership responsibilities include developing and delivering all NERC related training and implementing processes and procedures associated with standards and requirements applicable to the Oxy Registered Entities for both O&P and CIP. She is on the NERC Members Representative Committee (MRC), Standards Committee (SC), Reliability and Security Technical Committee (RSTC) and is the North American Generator Forum (NAGF) Secretary. She is also a member of the Project 2019-06 Cold Weather Standard Drafting team. She holds a Bachelor of Science degree in Cyber Security Policy and Management from University of Maryland University College.

Agenda Item 5
Standards Committee
January 20, 2021

Project 2019-06 Cold Weather

Action

Authorize initial posting of proposed Reliability Standards EOP-011-2, IRO-010-4 and TOP-003-5 and associated Implementation Plan for a 45-day formal comment period, with ballot pool formed in the first 30 days, and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period.

Background

In July 2019, the FERC and NERC staff report titled The South Central United States Cold Weather Bulk Electronic System Event of January 17, 2018 (Report) was released. Following the report, Southwest Power Pool, Inc. (SPP) submitted a SAR proposing a new standard development project to review and address the recommendations in the Report. The industry need for this SAR according to SPP is to enhance the reliability of the BES during cold weather events. On September 24, 2020, the Standards Committee accepted the Standards Authorization Request (SAR) and authorized the SAR DT to become the standards drafting team (SDT). The SDT made modifications in EOP-011-2, IRO-010-4, and TOP-003-5.

A quality review (QR) on the SDT documents was performed November 30 – December 4, 2020. NERC Staff included Lauren Perotti, Marisa Hecht, Kiel Lyons, Alexander Kaplen, and James McGrane. Industry QR members were Andrea Koch (EEI), and Sean Bodkin (Dominion). The SDT considered all QR inputs and revised the proposed standard where appropriate. Matt Harward, the SDT chair, approved the final documents before submission to the Standards Committee to request authorization for a 45-day initial comment period and ballot.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 5a
Standards Committee
January 20, 2021

Implementation Plan

Project 2019-06 Cold Weather

Applicable Standard(s)

- EOP-011-2 – Emergency Preparedness
- IRO-010-4 – Reliability Coordinator Data Specification and Collection
- TOP-003-5 – Operational Reliability Data

Requested Retirement(s)

- EOP-011-1 – Emergency Operations
- IRO-010-3 – Reliability Coordinator Data Specification and Collection
- TOP-003-4 – Operational Reliability Data

Applicable Entities

- See subject Reliability Standards.

Background

In July 2019, FERC and NERC staff released a joint report titled *The South Central United States Cold Weather Bulk Electronic System Event of January 17, 2018*[1]. Following the publication of the report, a Standard Authorization Request[2] was submitted to review and address the recommendations in the report, including:

1. Generator Owner or Generator Operator develops and implements cold weather preparedness plans, procedures, and awareness training based on factors such as geographical location and plant configurations, which may include:
   a. The need for accurate cold weather temperature design specifications or historical demonstrated performance and operating limitations during cold weather;
   b. Implementing freeze protection measures; and
   c. Performing periodic maintenance and inspection of freeze protection measures.
2. Balancing Authority, Reliability Coordinators, or Transmission Operators, as applicable will include in its data specifications that the Generator Owner or Generator Operator will provide its BES generating unit's associated design specification or historical demonstrated performance and operating limitations during cold weather.

[1] Link to report: https://www.nerc.com/pa/rrm/ea/Documents/South_Central_Cold_Weather_Event_FERC-NERC-Report_20190718.pdf
[2] Link to SAR: https://www.nerc.com/pa/Stand/Project%20201906%20Cold%20Weather%20DL/2019-06_Cold_Weather_SAR_Clean_02192020.pdf

3. Balancing Authority, Reliability Coordinators, or Transmission Operators, as applicable will include in their data specifications that the Generator Owner or Generator Operator will provide a notification when local forecasted cold weather conditions are expected to limit BES generating unit capability or availability.
4. Reliability Coordinators, Balancing Authorities, and Transmission Operator incorporates the data, as communicated in deliverable #2 and #3 above, to perform their respective Operational Planning Analysis, develop their Operating Plans, or determine the expected availability of contingency reserves for the appropriate next day operating horizon.

The Reliability Standard revisions proposed by this project will help enhance the reliability of the Bulk Power System during cold weather events, and mitigate the potential for generating unit unavailability due to lack of preparation for cold weather periods by providing increased visibility of cold weather related data to the Reliability Coordinators, Balancing Authorities, and Transmission Operators, and by requiring a baseline level of cold weather planning and preparation by Generator Owners.

General Considerations

This implementation plan provides that entities shall have twelve months to become compliant with the revised Reliability Standards. This implementation plan reflects consideration that entities will need time to develop, implement, and maintain cold weather preparedness plan(s) for its generating site(s) under Reliability Standard EOP-011-2. This implementation plan also reflects consideration that entities will need time to develop, and distribute revised data specifications to affected entities, revised data specifications and for receiving entities to develop the necessary capabilities in order to comply with revised data specifications.

Effective Dates

Reliability Standard EOP-011-2

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Reliability Standard IRO-010-4

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Reliability Standard TOP-003-5

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Dates

Reliability Standard EOP-011-1

Reliability Standard EOP-011-1 shall be retired immediately prior to the effective date of Reliability Standard EOP-011-2 in the particular jurisdiction in which the revised Reliability Standard is becoming effective.

Reliability Standard IRO-010-3

Reliability Standard IRO-010-3 shall be retired immediately prior to the effective date of Reliability Standard IRO-010-4 in the particular jurisdiction in which the revised Reliability Standard is becoming effective.

Reliability Standard TOP-003-4

Reliability Standard TOP-003-4 shall be retired immediately prior to the effective date of Reliability Standard TOP-003-5 in the particular jurisdiction in which the revised Reliability Standard is becoming effective.

Initial Performance of Periodic Requirements

Responsible Entities shall develop, maintain, and implement the Operating Plan(s) required by Reliability Standard EOP-011-2 by the effective date of the Reliability Standard. For the cold weather preparedness plan(s) for generating unit(s) required under Requirement R7, the Responsible Entity shall perform annual maintenance and inspection of generating unit freeze protection measures under Requirement R7 Part 7.2 and conduct awareness training on the roles and responsibilities of personnel under Requirement R7 Part 7.4 by the effective date of the Reliability Standard.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal a 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR) for posting	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020

Anticipated Actions	Date
45-day initial formal comment period with ballot	January 2021
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** Reliability Coordinator Data Specification and Collection

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

3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area.

4. **Applicability**

   4.1. Reliability Coordinator.

   4.2. Balancing Authority.

   4.3. Generator Owner.

   4.4. Generator Operator.

   4.5. Transmission Operator.

   4.6. Transmission Owner.

   4.7. Distribution Provider.

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.

1.4. A periodicity for providing data.

1.5. The deadline by which the respondent is to provide the indicated data.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification for data.

R2. The Reliability Coordinator shall distribute its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

M2. The Reliability Coordinator shall make available evidence that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R3. Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: *(Violation Risk Factor: Medium) (Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations)*

3.1 A mutually agreeable format

3.2 A mutually agreeable process for resolving data conflicts

3.3 A mutually agreeable security protocol

M3. The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the 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 Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Reliability Coordinator shall retain its dated, current, in force documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

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.

1.4. Additional Compliance Information: None.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include two or fewer of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
						monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
				Assessments.	Real-time Assessments.	Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow one of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow two of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow any of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-2. Docket No. RD20-4-000	
4	TBD	Adopted by NERC Board of Trustees	Revisions under Project 2019-06

Agenda Item 5b
Standards Committee
January 20, 2021

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal a 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR) for posting	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020

Anticipated Actions	Date
45-day initial formal comment period with ballot	January 2021
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** Reliability Coordinator Data Specification and Collection

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

3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area.

4. **Applicability**

   4.1. Reliability Coordinator.

   4.2. Balancing Authority.

   4.3. Generator Owner.

   4.4. Generator Operator.

   4.5. Transmission Operator.

   4.6. Transmission Owner.

   4.7. Distribution Provider.

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to: *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

1.2. Provisions for notification of current Protection System and ~~Special Protection System~~ Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.

~~**1.2.**~~**1.4.** A periodicity for providing data.

~~**1.3.**~~**1.5.** The deadline by which the respondent is to provide the indicated data.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification for data.

R2. The Reliability Coordinator shall distribute its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *(Violation Risk Factor: Low) (Time Horizon: Operations Planning)*

M2. The Reliability Coordinator shall make available evidence that it has distributed its data specification to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. This evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R3. Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: *(Violation Risk Factor: Medium) (Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations)*

3.1 A mutually agreeable format

3.2 A mutually agreeable process for resolving data conflicts

3.3 A mutually agreeable security protocol

M3. The Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall make available evidence that it satisfied the obligations of the documented specification using the specified criteria. Such evidence could include but is not limited to electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” ~~As defined in the NERC Rules of Procedure, “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 the mandatory and enforceable ~~NERC~~ Reliability Standards in their respective jurisdictions.

1.2. ~~Data~~ 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 Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Reliability Coordinator shall retain its dated, current, in force documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.

The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its data specification to entities that have data required by the Reliability Coordinator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.

Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

~~The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~1.2.~~1.3. Compliance Monitoring and ~~Assessment Processes~~Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and ~~Assessment Processes~~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.

~~1.3.~~1.4. Additional Compliance Information: None.

Table of Compliance Elements

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include two or fewer ~~one~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include three~~two~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four~~three~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
						monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and	The Reliability Coordinator did not distribute its data specification as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
				Assessments.	Real-time Assessments.	Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow one of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow two of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 satisfied the obligations of the documented specifications for data but failed to follow any of the criteria shown in Parts 3.1 – 3.3.	The responsible entity receiving a data specification in Requirement R2 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None

E. Interpretations

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-2. Docket No. RD20-4-000	
4	TBD	Adopted by NERC Board of Trustees	Revisions under Project 2019-06

~~Guidelines and Technical Basis~~

~~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 adoption, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Definitions:~~

~~Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.~~

~~Rationale for Applicability Changes:~~

~~Changes were made to applicability based on IRO FYRT recommendation to address the need for UVLS and UFLS information in the data specification.~~

~~The Interchange Authority was removed because activities in the Coordinate Interchange standards are performed by software systems and not a responsible entity. The software, not a functional entity, performs the task of accepting and disseminating interchange data between entities. The Balancing Authority is the responsible functional entity for these tasks.~~

~~The Planning Coordinator and Transmission Planner were removed from Draft 2 as those entities would not be involved in a data specification concept as outlined in this standard.~~

~~Rationale:~~

~~Proposed Requirement R1, Part 1.1:~~

~~Is in response to issues raised in NOPR paragraph 67 on the need for obtaining non-BES and external network data necessary for the Reliability Coordinator to fulfill its responsibilities.~~

~~Proposed Requirement R1, Part 1.2:~~

~~Is in response to NOPR paragraph 78 on relay data.~~

~~Proposed Requirement R3, Part 3.3:~~

~~Is in response to NOPR paragraph 92 where concerns were raised about data exchange through secured networks.~~

~~Corresponding changes have been made to proposed TOP-003-3.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title: Operational Reliability Data**

2. **Number: TOP-003-5**

3. **Purpose:** To ensure that the Transmission Operator and Balancing Authority have data needed to fulfill their operational and planning responsibilities.

4. **Applicability:**

   4.1. Transmission Operator

   4.2. Balancing Authority

   4.3. Generator Owner

   4.4. Generator Operator

   4.5. Transmission Owner

   4.6. Distribution Provider

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.

1.2. Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.

1.4. A periodicity for providing data.

1.5. The deadline by which the respondent is to provide the indicated data.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification for data.

R2. Each Balancing Authority shall maintain a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring.

2.2. Provisions for notification of current Protection System and Remedial Action Scheme status or degradation that impacts System reliability.

2.3. A periodicity for providing data.

2.4. The deadline by which the respondent is to provide the indicated data.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification for data.

R3. Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R4. Each Balancing Authority shall distribute its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Each Balancing Authority shall make available evidence that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.

R5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

5.1. A mutually agreeable format

5.2. A mutually agreeable process for resolving data conflicts

5.3. A mutually agreeable security protocol

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specifications. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

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

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

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

Each Transmission Operator shall retain its dated, current, in force, documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring in accordance with Requirement R2 and Measurement M2 as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring in accordance with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

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.

1.4. Additional Compliance Information

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Transmission Operator did not include two or fewer of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification for the data necessary for it to perform its

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R2	Operations Planning	Lower	The Balancing Authority did not include one of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include two of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. OR, The Balancing Authority did not have a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
For the Requirement R3 and R4 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Lower	The Transmission Operator did not distribute its data specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its data specification to two entities, or more than 5% and less than or equal to10% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its data specification to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not distribute its data specification to four or more entities, or more than 15% of the entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R4	Operations Planning	Lower	The Balancing Authority did not distribute its data specification to one entity, or 5% or less of the entities,	The Balancing Authority did not distribute its data specification to two entities, or more than 5% and less than or	The Balancing Authority did not distribute its data specification to three entities, or more than 10% and less than or	The Balancing Authority did not distribute its data specification to four or more entities, or more than 15% of the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	equal to 10% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	equal to 15% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring.
R5	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet one of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet two of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet three of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP-003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of proposed standard for formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title: Operational Reliability Data**

2. **Number: TOP-003-5~~4~~**

3. **Purpose:** To ensure that the Transmission Operator and Balancing Authority have data needed to fulfill their operational and planning responsibilities.

4. **Applicability:**

   4.1. Transmission Operator

   4.2. Balancing Authority

   4.3. Generator Owner

   4.4. Generator Operator

   4.5. Transmission Owner

   4.6. Distribution Provider

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.

1.2. Provisions for notification of current Protection System and ~~Special Protection System~~ Remedial Action Scheme (RAS) status or degradation that impacts System reliability.

~~1.2.~~1.3. Provisions for notification of BES generating unit-specific design specification or minimum historical performance during cold weather, and expected BES generating unit operation limitations during local forecasted cold weather.

~~1.3.~~1.4. A periodicity for providing data.

~~1.4.~~1.5. The deadline by which the respondent is to provide the indicated data.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification for data.

R2. Each Balancing Authority shall maintain a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. The data specification shall include, but not be limited to: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions and Real-time monitoring.

2.2. Provisions for notification of current Protection System and ~~Special Protection System~~ Remedial Action Scheme status or degradation that impacts System reliability.

2.3. A periodicity for providing data.

2.4. The deadline by which the respondent is to provide the indicated data.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification for data.

R3. Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or e-mail records.

R4. Each Balancing Authority shall distribute its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Each Balancing Authority shall make available evidence that it has distributed its data specification to entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring. Such evidence could include but is not limited to web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, or e-mail records.

R5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]*

5.1. A mutually agreeable format

5.2. A mutually agreeable process for resolving data conflicts

5.3. A mutually agreeable security protocol

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations of the documented specifications. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” ~~As defined in the NERC Rules of Procedure, “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 ~~the NERC~~ Reliability Standards in their respective jurisdictions.

~~1.2. Data~~ Evidence Retention:

~~1.3.~~1.2. The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each responsible entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

Each Transmission Operator shall retain its dated, current, in force, documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.

Each Balancing Authority shall retain its dated, current, in force, documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring in accordance with Requirement R2 and Measurement M2 as well as any documents in force since the last compliance audit.

Each Transmission Operator shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Transmission Operator’s Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.

Each Balancing Authority shall retain evidence for three calendar years that it has distributed its data specification to entities that have data required by the Balancing Authority’s analysis functions and Real-time monitoring in accordance with Requirement R4 and Measurement M4.

Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall retain evidence for the most recent

90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

~~If a responsible entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or the time period specified above, whichever is longer.~~

~~The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~1.4.~~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.

~~1.5.~~1.4. **Additional Compliance Information**

None.

-Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Transmission Operator did not include two or fewer~~one~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include ~~two~~three of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include four~~three~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any~~four~~ of the parts (Part 1.1 through Part 1.5~~4~~) of the documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Lower	The Balancing Authority did not include one of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include two of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.4) of the documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring. OR, The Balancing Authority did not have a documented specification for the data necessary for it to perform its analysis functions and Real-time monitoring.
For the Requirement R3 and R4 VSLs only, the intent of the SDT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						
R3	Operations Planning	Lower	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data	The Transmission Operator did not distribute its data

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to two entities, or more than 5% and less than or equal to10% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	specification to four or more entities, or more than 15% of the entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R4	Operations Planning	Lower	The Balancing Authority did not distribute its data specification to one entity, or 5% or less of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to two entities, or more than 5% and less than or equal to 10% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to three entities, or more than 10% and less than or equal to 15% of the entities, whichever is greater, that have data required by the Balancing Authority's analysis functions and Real-time monitoring.	The Balancing Authority did not distribute its data specification to four or more entities, or more than 15% of the entities that have data required by the Balancing Authority's analysis functions and Real-time monitoring.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet one of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet two of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 satisfied the obligations in the data specification but did not meet three of the criteria shown in Requirement R5 (Parts 5.1 – 5.3).	The responsible entity receiving a data specification in Requirement R3 or R4 did not satisfy the obligations of the documented specifications for data.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP-003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07

~~Guidelines and Technical Basis~~

~~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 Definitions:~~

~~Changes made to the proposed definitions were made in order to respond to issues raised in NOPR paragraphs 55, 73, and 74 dealing with analysis of SOLs in all time horizons, questions on Protection Systems and Special Protection Systems in NOPR paragraph 78, and recommendations on phase angles from the SW Outage Report (recommendation 27). The intent of such changes is to ensure that Real-time Assessments contain sufficient details to result in an appropriate level of situational awareness. Some examples include: 1) analyzing phase angles which may result in the implementation of an Operating Plan to adjust generation or curtail transactions so that a Transmission facility may be returned to service, or 2) evaluating the impact of a modified Contingency resulting from the status change of a Special Protection Scheme from enabled/in-service to disabled/out-of-service.~~

~~Rationale for R1:~~

~~Changes to proposed Requirement R1, Part 1.1 are in response to issues raised in NOPR paragraph 67 on the need for obtaining non-BES and external network data necessary for the Transmission Operator to fulfill its responsibilities.~~

~~Proposed Requirement R1, Part 1.2 is in response to NOPR paragraph 78 on relay data. The language has been moved from approved PRC-001-1.~~

~~Corresponding changes have been made to Requirement R2 for the Balancing Authority and to proposed IRO-010-2, Requirement R1 for the Reliability Coordinator.~~

~~Rationale for R5:~~

~~Proposed Requirement R5, Part 5.3 is in response to NOPR paragraph 92 where concerns were raised about data exchange through secured networks.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of the proposed standard for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** **Emergency Preparedness**

2. **Number:** **EOP-011-2**

3. **Purpose:** To ensure each Transmission Operator, Balancing Authority, and Generator Owner has developed plan(s) to mitigate and prepare for operating Emergencies; and that Operating Plans are coordinated within a Reliability Coordinator Area.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Reliability Coordinator

   4.1.3 Transmission Operator

   4.1.4 Generator Owner

   4.2. Facilities

   4.2.1 For the purpose of this standard, the term "generating unit" includes all BES generating units and BES generating plants.

5. **Effective Date:** See Implementation Plan for Project 2019-06.

B. Requirements and Measures

R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

1.1. Roles and responsibilities for activating the Operating Plan(s);

1.2. Processes to prepare for and mitigate Emergencies including:

1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;

1.2.2. Cancellation or recall of Transmission and generation outages;

1.2.3. Transmission system reconfiguration;

1.2.4. Redispatch of generation request;

1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

1.2.6. Reliability impacts of:

1.2.6.1. cold weather conditions; and

1.2.6.2. any other extreme weather conditions.

M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.

R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

2.1. Roles and responsibilities for activating the Operating Plan(s);

2.2. Processes to prepare for and mitigate Emergencies including:

2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;

2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;

2.2.3. Managing generating resources in its Balancing Authority Area to address:

2.2.3.1. capability and availability;

2.2.3.2. fuel supply and inventory concerns;

2.2.3.3. fuel switching capabilities; and

2.2.3.4. environmental constraints.

2.2.4. Public appeals for voluntary Load reductions;

2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;

2.2.6. Reduction of internal utility energy use;

2.2.7. Use of Interruptible Load, curtailable Load and demand response;

2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

2.2.9. Reliability impacts of:

2.2.9.1. cold weather conditions; and

2.2.9.2. any other extreme weather conditions.

M2. Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.

R3. The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. Within 30 calendar days of receipt, the Reliability Coordinator shall:

3.1.1. Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;

3.1.2. Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and

3.1.3. Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.

M3. The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.

R4. Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*

M4. The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

R5. Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .

R6. Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M6. Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.

R7. Each Generator Owner shall develop, maintain, and implement one or more cold weather preparedness plan(s) for its generating unit(s). The cold weather preparedness plan(s) shall include the following, at a minimum: *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-Time Operations]*

7.1. Generating unit(s) freeze protection measures based on unique factors such as geographical location and plant configuration;

7.2. Annual maintenance and inspection of generating unit(s) freeze protection measures;

7.3. Generating unit(s) cold weather data, to include:

7.3.1. Generating unit(s) operating limitations in cold weather; and

7.3.2. Generating unit(s):

7.3.2.1. minimum design temperature; or

7.3.2.2. minimum demonstrated historical performance during cold weather in the previous 5 years;

7.4. Awareness training on the roles and responsibilities of site personnel contained in the cold weather preparedness plan.

M7. Each Generator Owner shall have a documented cold weather preparedness plan in accordance with Requirement R7; and have evidence such as a review or revision history to indicate that the plan has been maintained; and have evidence such as operator checklists, work orders, test records, other operating and maintenance documentation, or other communication documentation to show that its cold weather preparedness plan was implemented; and have evidence such as training materials and attendance list showing successful completion of training.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Evidence Retention

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

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

- The Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.
- The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.
- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.

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.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission s Operator Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	The Balancing Authority developed an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	The Balancing Authority failed to develop an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator within 30 calendar days.	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit tis Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency	The Reliability Coordinator that received an Emergency

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					notification from a Transmission Operator or Balancing Authority did notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators but failed to notify within 30 minutes from the time of receiving notification.	notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	Operations Planning and Real-time Operations	High	The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.	The Generator Owner developed a cold weather preparedness plan(s) but failed to maintain it. OR The Generator Owner's cold weather preparedness plan failed to include two of the applicable requirement Parts within Requirement R7.	The Generator Owner developed and maintained a cold weather preparedness plan(s) but failed to fully implement it. OR The Generator Owner's cold weather preparedness plan failed to include three of the applicable requirement Parts within Requirement R7.	The Generator Owner does not have a cold weather preparedness plan. OR The Generator Owner has a cold weather preparedness plan, but failed to include all the applicable requirement Parts within Requirement R7.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
2	TBD	Adopted by the Board of Trustees	Revised under Project 2019-06

Attachment 1-EOP-011-2
Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

1. **Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.
2. **Notification**. A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. **EEA 1 — All available generation resources in use.**

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.
- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. **EEA 2 — Load management procedures in effect**.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities **and market participants**. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators**.**

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it’s possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA**.**

0.1 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of the proposed standard for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standards Authorization Request (SAR)	July 22, 2020
SAR posted for comment	February 19 – March 19, 2020
SAR posted for comment	April 22 – May 21, 2020
45-day initial formal comment period with ballot	January 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 2021
45-day formal comment period with additional ballot	July 2021
10-day final ballot	October 1 – 11, 2021
NERC Board (Board) adoption	November 2021

A. Introduction

1. **Title:** **Emergency Preparedness ~~Operations~~**

2. **Number:** **EOP-011-2~~1~~**

3. **Purpose:** To ~~effects of operating Emergencies by~~ ensure~~ing~~ each Transmission Operator, ~~and~~ Balancing Authority, and Generator Owner has developed ~~Operating P~~plan(s) to mitigate and prepare for operating Emergencies;~~,~~ and that ~~those~~ Operating ~~p~~Plans are coordinated within a Reliability Coordinator Area.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Reliability Coordinator

   4.1.3 Transmission Operator

   4.1.4 Generator Owner

   4.2. Facilities

   4.2.1 For the purpose of this standard, the term "generating unit" includes all BES generating units and BES generating plants.

5. **Effective Date:** See Implementation Plan for ~~EOP-011-1~~Project 2019-06.

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

~~EOP-011-1 consolidates requirements from three standards: EOP-001-2.1b, EOP-002-3.1, and EOP-003-2.~~

~~The standard streamlines the requirements for Emergency operations for the Bulk Electric System into a clear and concise standard that is organized by Functional Entity. In addition, the revisions clarify the critical requirements for Emergency Operations, while ensuring strong communication and coordination across the Functional Entities.~~

B. Requirements and Measures

R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

1.1. Roles and responsibilities for activating the Operating Plan(s);

1.2. Processes to prepare for and mitigate Emergencies including:

1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;

1.2.2. Cancellation or recall of Transmission and generation outages;

1.2.3. Transmission system reconfiguration;

1.2.4. Redispatch of generation request;

1.2.5. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

1.2.6. Reliability impacts of:

1.2.6.1. cold weather conditions; and

~~1.2.5.1.~~1.2.6.2. any other extreme weather conditions.

M1. Each Transmission Operator will have a dated Operating Plan(s) developed in accordance with Requirement R1 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R1.

R2. Each Balancing Authority shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area. The Operating Plan(s) shall include the following, as applicable: *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]*

2.1. Roles and responsibilities for activating the Operating Plan(s);

2.2. Processes to prepare for and mitigate Emergencies including:

2.2.1. Notification to its Reliability Coordinator, to include current and projected conditions when experiencing a Capacity Emergency or Energy Emergency;

2.2.2. Requesting an Energy Emergency Alert, per Attachment 1;

2.2.3. Managing generating resources in its Balancing Authority Area to address:

2.2.3.1. capability and availability;

2.2.3.2. fuel supply and inventory concerns;

2.2.3.3. fuel switching capabilities; and

2.2.3.4. environmental constraints.

2.2.4. Public appeals for voluntary Load reductions;

2.2.5. Requests to government agencies to implement their programs to achieve necessary energy reductions;

2.2.6. Reduction of internal utility energy use;

2.2.7. Use of Interruptible Load, curtailable Load and demand response;

2.2.8. Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and

2.2.9. Reliability impacts of:

2.2.9.1. cold weather conditions; and

~~2.2.8.1.~~2.2.9.2. any other extreme weather conditions.

M2. Each Balancing Authority will have a dated Operating Plan(s) developed in accordance with Requirement R2 and reviewed by its Reliability Coordinator; evidence such as a review or revision history to indicate that the Operating Plan(s) has been maintained; and will have as evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its Operating Plan(s) was implemented for times when an Emergency has occurred, in accordance with Requirement R2.

R3. The Reliability Coordinator shall review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. Within 30 calendar days of receipt, the Reliability Coordinator shall:

3.1.1. Review each submitted Operating Plan(s) on the basis of compatibility and inter-dependency with other Balancing Authorities' and Transmission Operators' Operating Plans;

3.1.2. Review each submitted Operating Plan(s) for coordination to avoid risk to Wide Area reliability; and

3.1.3. Notify each Balancing Authority and Transmission Operator of the results of its review, specifying any time frame for resubmittal of its Operating Plan(s) if revisions are identified.

M3. The Reliability Coordinator will have documentation, such as dated e-mails or other correspondences that it reviewed Transmission Operator and Balancing Authority Operating Plans within 30 calendar days of submittal in accordance with Requirement R3.

R4. Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. *[Violation Risk Factor: High] [Time Horizon: Operation Planning]*

M4. The Transmission Operator and Balancing Authority will have documentation, such as dated emails or other correspondence, with an Operating Plan(s) version history showing that it responded and updated the Operating Plan(s) within the timeframe identified by its Reliability Coordinator in accordance with Requirement R4.

R5. Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority within its Reliability Coordinator Area shall notify, within 30 minutes from the time of receiving notification, other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M5. Each Reliability Coordinator that receives an Emergency notification from a Balancing Authority or Transmission Operator within its Reliability Coordinator Area will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that will be used to determine if the Reliability Coordinator communicated, in accordance with Requirement R5, with other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators .

R6. Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1. *[Violation Risk Factor: High] [Time Horizon: Real-Time Operations]*

M6. Each Reliability Coordinator, with a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area, will have, and provide upon request, evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent evidence that it declared an Energy Emergency Alert, as detailed in Attachment 1, in accordance with Requirement R6.

R7. Each Generator Owner shall develop, maintain, and implement one or more cold weather preparedness plan(s) for its generating unit(s). The cold weather preparedness plan(s) shall include the following, at a minimum: *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-Time Operations]*

7.1. Generating unit(s) freeze protection measures based on unique factors such as geographical location and plant configuration;

7.2. Annual maintenance and inspection of generating unit(s) freeze protection measures;

7.3. Generating unit(s) cold weather data, to include:

7.3.1. Generating unit(s) operating limitations in cold weather; and

7.3.2. Generating unit(s):

7.3.2.1. minimum design temperature; or

7.3.2.2. minimum demonstrated historical performance during cold weather in the previous 5 years;

7.4. Awareness training on the roles and responsibilities of site personnel contained in the cold weather preparedness plan.

M7. Each Generator Owner shall have a documented cold weather preparedness plan in accordance with Requirement R7; and have evidence such as a review or revision history to indicate that the plan has been maintained; and have evidence such as operator checklists, work orders, test records, other operating and maintenance documentation, or other communication documentation to show that its cold weather preparedness plan was implemented; and have evidence such as training materials and attendance list showing successful completion of training.

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, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with the mandatory and enforceable ~~NERC~~ Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

~~The Balancing Authority, Reliability Coordinator, and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation. 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 following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

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

- The Transmission Operator shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R1 and R4 and Measures M1 and M4.
- The Balancing Authority shall retain the current Operating Plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirements R2 and R4, and Measures M2 and M4.
- The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.
- The Generator Owner shall retain the cold weather preparedness plan(s), evidence of review or revision history plus each version issued since the last audit and evidence of compliance since the last audit for Requirement R7 and Measure M7.

~~If a Balancing Authority, Reliability Coordinator or Transmission Operator is found non-compliant, it shall keep information related to the non-compliance until found compliant.~~

~~The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~1.5.~~1.3. Compliance Monitoring and ~~Assessment Processes~~Enforcement Program:

As defined in the NERC Rules of Procedure; "Compliance Monitoring and ~~Assessment~~ Enforcement ~~Processes~~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 ~~r~~Reliability ~~s~~Standard.

~~1.6. Additional Compliance Information~~

~~None~~

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to maintain it.	The Transmission Operator developed an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area but failed to have it reviewed by its Reliability Coordinator.	The Transmission Operator failed to develop an Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. OR The Transmission Operator developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission s Operator Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Real-time Operations, Operations Planning, Long-term Planning	High	N/A	The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to maintain it.	The Balancing Authority developed an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to have it reviewed by its Reliability Coordinator.	The Balancing Authority failed to develop an Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area. OR The Balancing Authority developed a Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies within its Balancing Authority Area but failed to implement it.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	High	N/A	N/A	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator within 30 calendar days.	The Reliability Coordinator identified a reliability risk but failed to notify the Balancing Authority or Transmission Operator.
R4	Operations Planning	High	N/A	N/A	The Transmission Operator or Balancing Authority failed to update and resubmit tis Operating Plan(s) to its Reliability Coordinator within the timeframe specified by its Reliability Coordinator.	The Transmission Operator or Balancing Authority failed to update and resubmit its Operating Plan(s) to its Reliability Coordinator.
R5	Real-time Operations	High	N/A	N/A	The Reliability Coordinator that received an Emergency	The Reliability Coordinator that received an Emergency

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					notification from a Transmission Operator or Balancing Authority did notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators but failed to notify within 30 minutes from the time of receiving notification.	notification from a Transmission Operator or Balancing Authority failed to notify neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators.
R6	Real-time Operations	High	N/A	N/A	N/A	The Reliability Coordinator that had a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area failed to declare an Energy Emergency Alert.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	Operations Planning and Real-time Operations	High	The Generator Owner's cold weather preparedness plan failed to include one of the applicable requirement Parts within Requirement R7.	The Generator Owner developed a cold weather preparedness plan(s) but failed to maintain it. OR The Generator Owner's cold weather preparedness plan failed to include two of the applicable requirement Parts within Requirement R7.	The Generator Owner developed and maintained a cold weather preparedness plan(s) but failed to fully implement it. OR The Generator Owner's cold weather preparedness plan failed to include three of the applicable requirement Parts within Requirement R7.	The Generator Owner does not have a cold weather preparedness plan. OR The Generator Owner has a cold weather preparedness plan, but failed to include all the applicable requirement Parts within Requirement R7.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by Board of Trustees	Merged EOP-001-2.1b, EOP-002-3.1 and EOP-003-2.
1	November 19, 2015	FERC approved EOP-011-1. Docket Nos. RM15-7-000, RM15-12-000, and RM15-13-000. Order No. 818	
2	TBD	Adopted by the Board of Trustees	Revised under Project 2019-06

Attachment 1-EOP-011-2~~1~~
Energy Emergency Alerts

Introduction

This Attachment provides the process and descriptions of the levels used by the Reliability Coordinator in which it communicates the condition of a Balancing Authority which is experiencing an Energy Emergency.

A. General Responsibilities

1. **Initiation by Reliability Coordinator.** An Energy Emergency Alert (EEA) may be initiated only by a Reliability Coordinator at 1) the Reliability Coordinator's own request, or 2) upon the request of an energy deficient Balancing Authority.
2. **Notification**. A Reliability Coordinator who declares an EEA shall notify all Balancing Authorities and Transmission Operators in its Reliability Coordinator Area. The Reliability Coordinator shall also notify all neighboring Reliability Coordinators.

B. EEA Levels

Introduction

To ensure that all Reliability Coordinators clearly understand potential and actual Energy Emergencies in the Interconnection, NERC has established three levels of EEAs. The Reliability Coordinators will use these terms when communicating Energy Emergencies to each other. An EEA is an Emergency procedure, not a daily operating practice, and is not intended as an alternative to compliance with NERC Reliability Standards.

The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. **EEA 1 — All available generation resources in use.**

Circumstances:

- The Balancing Authority is experiencing conditions where all available generation resources are committed to meet firm Load, firm transactions, and reserve commitments, and is concerned about sustaining its required Contingency Reserves.

- Non-firm wholesale energy sales (other than those that are recallable to meet reserve requirements) have been curtailed.

2. **EEA 2 — Load management procedures in effect**.

Circumstances:

- The Balancing Authority is no longer able to provide its expected energy requirements and is an energy deficient Balancing Authority.
- An energy deficient Balancing Authority has implemented its Operating Plan(s) to mitigate Emergencies.

- An energy deficient Balancing Authority is still able to maintain minimum Contingency Reserve requirements.

During EEA 2, Reliability Coordinators and energy deficient Balancing Authorities have the following responsibilities:

2.1 Notifying other Balancing Authorities **and market participants**. The energy deficient Balancing Authority shall communicate its needs to other Balancing Authorities and market participants. Upon request from the energy deficient Balancing Authority, the respective Reliability Coordinator shall post the declaration of the alert level, along with the name of the energy deficient Balancing Authority on the RCIS website.

2.2 Declaration period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 2 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities and Transmission Operators**.**

2.3 Sharing information on resource availability. Other Reliability Coordinators of Balancing Authorities with available resources shall coordinate, as appropriate, with the Reliability Coordinator that has an energy deficient Balancing Authority.

2.4 Evaluating and mitigating Transmission limitations. The Reliability Coordinator shall review Transmission outages and work with the Transmission Operator(s) to see if it's possible to return to service any Transmission Elements that may relieve the loading on System Operating Limits (SOLs) or Interconnection Reliability Operating Limits (IROLs).

2.5 Requesting Balancing Authority actions. Before requesting an EEA 3, the energy deficient Balancing Authority must make use of all available resources; this includes, but is not limited to:

2.5.1 All available generation units are on line. All generation capable of being on line in the time frame of the Emergency is on line.

2.5.2 Demand-Side Management. Activate Demand-Side Management within provisions of any applicable agreements.

3. EEA 3 —Firm Load interruption is imminent or in progress.

Circumstances:

- The energy deficient Balancing Authority is unable to meet minimum Contingency Reserve requirements.

During EEA 3, Reliability Coordinators and Balancing Authorities have the following responsibilities:

3.1 Continue actions from EEA 2. The Reliability Coordinators and the energy deficient Balancing Authority shall continue to take all actions initiated during EEA 2.

3.2 Declaration Period. The energy deficient Balancing Authority shall update its Reliability Coordinator of the situation at a minimum of every hour until the EEA 3 is terminated. The Reliability Coordinator shall update the energy deficiency information posted on the RCIS website as changes occur and pass this information on to the neighboring Reliability Coordinators, Balancing Authorities, and Transmission Operators.

3.3 Reevaluating and revising SOLs and IROLs. The Reliability Coordinator shall evaluate the risks of revising SOLs and IROLs for the possibility of delivery of energy to the energy deficient Balancing Authority. Reevaluation of SOLs and IROLs shall be coordinated with other Reliability Coordinators and only with the agreement of the Transmission Operator whose Transmission Owner (TO) equipment would be affected. SOLs and IROLs shall only be revised as long as an EEA 3 condition exists, or as allowed by the Transmission Owner whose equipment is at risk. The following are minimum requirements that must be met before SOLs or IROLs are revised:

3.3.1 Energy deficient Balancing Authority obligations. The energy deficient Balancing Authority, upon notification from its Reliability Coordinator of the situation, it will immediately take whatever actions are necessary to mitigate any undue risk to the Interconnection. These actions may include Load shedding.

3.4 Returning to pre-Emergency conditions. Whenever energy is made available to an energy deficient Balancing Authority such that the Systems can be returned to its pre-Emergency SOLs or IROLs condition, the energy deficient Balancing Authority shall request the Reliability Coordinator to downgrade the alert level.

3.4.1 Notification of other parties. Upon notification from the energy deficient Balancing Authority that an alert has been downgraded, the Reliability Coordinator shall notify the neighboring Reliability Coordinators (via the RCIS), Balancing Authorities and Transmission Operators that its Systems can be returned to its normal limits.

Alert 0 - Termination. When the energy deficient Balancing Authority is able to meet its Load and Operating Reserve requirements, it shall request its Reliability Coordinator to terminate the EEA**.**

0.1 Notification. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS of the termination. The Reliability Coordinator shall also notify the neighboring Balancing Authorities and Transmission Operators.

~~Guidelines and Technical Basis~~

~~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 R1:~~

~~The EOP SDT examined the recommendation of the EOP Five-Year Review Team (FYRT) and FERC directive to provide guidance on applicable entity responsibility that was included in EOP-001-2.1b. The EOP SDT removed EOP-001-2.1b, Attachment 1, and incorporated it into this standard under the applicable requirements. This also establishes a separate requirement for the Transmission Operator to create an Operating Plan(s) for mitigating operating Emergencies in its Transmission Operator Area.~~

~~The Operating Plan(s) can be one plan, or it can be multiple plans.~~

~~"Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency" was retained. This is a process in the plan(s) that determines when the Transmission Operator must notify its Reliability Coordinator.~~

~~To meet the associated measure, an entity would likely provide evidence that such an evaluation was conducted along with an explanation of why any overlap of Loads between manual and automatic load shedding was unavoidable or reasonable.~~

~~An Operating Plan(s) is implemented by carrying out its stated actions.~~

~~If any Parts of Requirement R1 are not applicable, the Transmission Operator should note "not applicable" in the Operating Plan(s). The EOP SDT recognizes that across the regions, Operating Plan(s) may not include all the elements listed in this requirement due to restrictions, other methods of managing situations, and documents that may already exist that speak to a process that already exists. Therefore, the entity must provide in the plan(s) that the element is not applicable and detail why it is not applicable for the plan(s).~~

~~With respect to automatic Load shedding schemes that include both UVLS and UFLS, the EOP SDT's intent is to keep manual and automatic Load shed schemes as separate as possible, but realizes that sometimes, due to system design, there will be overlap. The intent in Requirement R1 Part 1.2.5. is to minimize, as much as possible, the use of manual Load shedding which is already armed for automatic Load shedding. The automatic Load shedding schemes are the important backstops against Cascading outages or System collapse. If any entity manually sheds a Load which was included in an automatic scheme, it reduces the effectiveness of that automatic scheme. Each entity should review their automatic Load shedding schemes and coordinate their manual processes so that any overlapping use of Loads is avoided to the extent reasonably possible.~~

~~Rationale for R2:~~

~~To address the recommendation of the FYRT and the FERC directive to provide guidance on applicable entity responsibility in EOP-001-2.1b, Attachment 1, the EOP SDT removed EOP-001-2.1b, Attachment 1, and incorporated it into this standard under the applicable requirements. EOP-011-1 also establishes a separate requirement for the Balancing Authority to create its Operating Plan(s) to address Capacity and Energy Emergencies.~~

~~The Operating Plan(s) can be one plan, or it can be multiple plans.~~

~~An Operating Plan(s) is implemented by carrying out its stated actions.~~

~~If any Parts of Requirement R2 are not applicable, the Balancing Authority should note "not applicable" in the Operating Plan(s). The EOP SDT recognizes that across the regions, Operating Plan(s) may not include all the elements listed in this requirement due to restrictions, other methods of managing situations, and documents that may already exist that speak to a process that already exists. Therefore, the entity must provide in the plan(s) that the element is not applicable and detail why it is not applicable for the plan(s).~~

~~The EOP SDT retained the statement "Operator-controlled manual Load shedding," as it was in the current EOP-003-2 and is consistent with the intent of the EOP SDT.~~

~~With respect to automatic Load shedding schemes that include both UVLS and UFLS, the EOP SDT's intent is to keep manual and automatic Load shedding schemes as separate as possible, but realizes that sometimes, due to system design, there will be overlap. The intent in Requirement R2 Part 2.2.8. is to minimize as much as possible the use manual Load shedding which is already armed for automatic Load shedding. The automatic Load shedding schemes are the important backstops against Cascading outages or System collapse. If an entity manually sheds a Load that was included in an automatic scheme, it reduces the effectiveness of that automatic scheme. Each entity should review its automatic Load shedding schemes and coordinate its manual processes so that any overlapping use of Loads is avoided to the extent possible.~~

~~The EOP SDT retained Requirement R8 from EOP-002-3.1 and added it to the Parts in Requirement R2.~~

~~Rationale for R3:~~

~~The SDT agreed with industry comments that the Reliability Coordinator does not need to approve BA and TOP plan(s). The SDT has changed this requirement to remove the approval but still require the RC to review each entity's plan(s), looking specifically for reliability risks. This is consistent with the Reliability Coordinator's role within the Functional Model and meets the FERC directive regarding the RC's involvement in Operating Plan(s) for mitigating Emergencies.~~

~~Rationale for Requirement R4:~~

~~Requirement R4 supports the coordination of Operating Plans within a Reliability Coordinator Area in order to identify and correct any Wide Area reliability risks. The EOP SDT expects the Reliability Coordinator to make a reasonable request for response time. The time period~~

~~requested by the Reliability Coordinator to the Transmission Operator and Balancing Authority to update the Operating Plan(s) will depend on the scope and urgency of the requested change.~~

~~Rationale for R5~~

~~The EOP SDT used the existing requirement in EOP-002-3.1 for the Balancing Authority and added the words "within 30 minutes from the time of receiving notification" to the requirement to communicate the intent that timeliness is important, while balancing the concern that in an Emergency there may be a need to alleviate excessive notifications on Balancing Authorities and Transmission Operators. By adding this time limitation, a measurable standard is set for when the Reliability Coordinator must complete these notifications.~~

~~Rationale for Introduction~~

~~LSEs were removed from Attachment 1, as an LSE has no Real-time reliability functionality with respect to EEAs.~~

~~EOP-002-3.1 Requirement R9 was in place to allow for a Transmission Service Provider to change the priority of a service request, as permitted in its transmission tariff, informing the Reliability Coordinator so that the service would not be curtailed by a TLR; and since the Tagging Specs did not allow profiles to be changed, this was the only method to accomplish it. Under NAESB WEQ E-tag Specification v1811 R3.6.1.3, this has been modified and now the TSP has the ability to change the Transmission priority which, in turn, is reflected in the IDC. This technology change allows for the deletion of Requirement R9 in its entirety. Requirement R9 meets with Criterion A of Paragraph 81 and should be retired.~~

~~Rationale for (2) Notification~~

~~The EOP SDT deleted the language, "*The Reliability Coordinator shall also notify all other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS). Additionally, conference calls between RCs shall be held as necessary to communicate system conditions. The RC shall also notify the other RCs when the alert has ended*" as duplicative to proposed IRO-014-3 Requirement R1:~~

~~R1. Each Reliability Coordinator shall have and implement Operating Procedures, Operating Processes, or Operating Plans, for activities that require notification or coordination of actions that may impact adjacent Reliability Coordinator Areas, to support Interconnection reliability. These Operating Procedures, Operating Processes, or Operating Plans shall include, but are not limited to, the following:~~

~~Communications and notifications, and the process to follow in making those notifications.~~

~~Energy and capacity shortages.~~

~~Control of voltage, including the coordination of reactive resources.~~

~~Exchange of information including planned and unplanned outage information to support its Operational Planning Analyses and Real-time Assessments.~~

~~Authority to act to prevent and mitigate system conditions which could adversely impact other Reliability Coordinator Areas.~~

~~Provisions for weekly conference calls.~~

~~Rationale for EEA 2:~~

~~The EOP SDT modified the "Circumstances" for EEA 2 to show that an entity will be in this level when it has implemented its Operating Plan(s) to mitigate Emergencies but is still able to maintain Contingency Reserves.~~

~~Rationale for EEA 3:~~

~~This rationale was added at the request of stakeholders asking for justification for moving a lack of Contingency Reserves into the EEA3 category.~~

~~The previous language in EOP-002-3.1, EEA 2 used "Operating Reserve," which is an all-inclusive term, including all reserves (including Contingency Reserves). Many Operating Reserves are used continuously, every hour of every day. Total Operating Reserve requirements are kind of nebulous since they do not have a specific hard minimum value. Contingency Reserves are used far less frequently. Because of the confusion over this issue, evidenced by the comments received, the drafting team thought that using minimum Contingency Reserve in the language would eliminate some of the confusion. This is a different approach but the drafting team believes this is a good approach and was supported by several commenters.~~

~~Using Contingency Reserves (which is a subset of Operating Reserves) puts a BA closer to the operating edge. The drafting team felt that the point where a BA can no longer maintain this important Contingency Reserves margin is a most serious condition and puts the BA into a position where they are very close to shedding Load ("imminent or in progress"). The drafting team felt that this warrants categorization at the highest level of EEA.~~

Agenda Item 6
Standards Committee
January 20, 2021

Project 2016-02 Modification to CIP Standards

Action

Authorize initial posting of proposed Reliability Standards CIP-002-7, CIP-003-9, CIP-004-7, CIP-005-8, CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7, CIP-010-5, CIP-011-3, and CIP-013-3, associated definitions, and Implementation Plan for a 45-day formal comment period, with ballot pool formed in the first 30 days, and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period.

Background

The proposed standards address the virtualization issue identified in the Project 2016-02 Standard Authorization Request (SAR), which the Standards Committee accepted on July 20, 2016. The SAR stated that the standard drafting team (SDT) should consider revisions to the CIP Reliability Standards and associated definitions to clarify the permitted architecture because of the increasing use of virtualization in industrial control system environments.

A quality review (QR) on the SDT documents was performed December 9, 2020 – January 4, 2021. NERC Staff included Marisa Hecht, Lauren Perotti, Daniel Bogle, and James McGrane. Industry QR members were Sean Bodkin (Dominion Energy), Andrea Koch and Mark Gray (EEI), and Morgan King (WECC). The SDT considered all QR inputs and revised the proposed standards where appropriate. The SDT co-chairs (Jay Cribb and Matt Hyatt) approved the final documents before submission to the Standards Committee to request authorization for a 45-day initial comment period and ballot.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda Item 6a
Standards Committee
January 20, 2021

CIP Definitions

Project 2016-02 Modifications to CIP Standards

This standards drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new glossary term. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in the redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber System Information (BCSI)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context~~, ESP names~~, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards~~, CIP-002 through CIP-011.~~
Cyber Asset	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: ~~•~~For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) ~~an~~ • ~~Electronic Security Perimeter~~the logical isolation, (2) a Physical Security Perimeter,~~ or~~ (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation ~~Electronic Security Perimeter(s)~~ of~~r~~ BES Cyber Systems. This includes Intermediate Systems.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	Proposal to retire.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System ~~that is outside of its associated Electronic Security Perimeter~~ via a bi-directional routable protocol connection.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	Proposal to retire.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed. ~~or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.~~
Intermediate Systems	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.~~A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface **New Definition**		A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Management Module New Definition		An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.
Management Systems New Definition		Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets that: • Are not logically isolated from a BES Cyber System; or • Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure, excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment. ~~connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.~~
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, or a ~~network within an ESP, or a~~ network that is not logically isolated from high or medium impact BES Cyber Systems. ~~Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System that performs one or more reliability tasks of a functional entity; • ~~- An Electronic Security Perimetert~~The logical isolation of a high or medium impact BES Cyber System; ~~or~~ • ~~-~~An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or • - Shared Cyber Infrastructure of a high or medium impact BES Cyber System
Self-Contained Application **New Definition**		Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.
Shared Cyber Infrastructure (SCI) **New Definition**		One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, ~~2.~~3. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems, ~~3.~~4. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and ~~4.~~5. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • Shared Cyber Infrastructure, • Network ~~within an Electronic Security Perimeter containingt~~ that is not logically isolated from high or medium impact BES Cyber Systems, or • Protected Cyber Asset associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Virtual Cyber Asset (VCA) **New Definition**		A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a Cyber Asset.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02 Virtualization Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Posting Document (Project 2016-02)”

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-6 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-2 – Cyber Security – Information Protection
- Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management
- Proposed terms for retirement listed in the "Definitions of Terms used in the above listed CIP Cyber Security Standards" document

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards and Definitions" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

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

- BES Cyber Asset (BCA)
- BES Cyber System
- BES Cyber System Information
- CIP Senior Manager
- Cyber Asset
- Cyber Security Incident
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate Systems (IS)
- Management Interface
- Management Module
- Management Systems
- Physical Access Control Systems
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Self-Contained Application
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the adoption to comply with the Revised CIP Standards and Definitions prior to the Effective Date.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions. Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until that date.

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the BES. Identification and categorization of BCS support appropriate protection against compromises 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-002-7:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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.

5. **Effective Date:** See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. RAS that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS or SCI that hosts any portion of a low impact BCS is not required).

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2. Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement	For Responsible Entities with more than a total of 40 BES assets in Requirement	For Responsible Entities with more than a total of 40 BES assets in Requirement	For Responsible Entities with more than a total of 40 BES assets in Requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, and associated SCI, five percent or fewer of identified BCS or associated SCI have not been categorized or have been	R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than five percent but	R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS and associated SCI, more than 10 percent but	R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than 15 percent of identified BCS or associated SCI have not been categorized or have been

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, five or fewer identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, and associated SCI, five percent or fewer high or medium BCS or associated SCI, have not been identified;	less than or equal to 10 percent of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BCS and associated SCI, more than five but less than or equal to 10 identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100	less than or equal to 15 percent of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS and associated SCI, more than 10 but less than or equal to 15 identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 15 identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than 15 percent of high or medium impact BCS or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, or associated SCI, five or fewer high or medium BCS or associated SCI, have not been identified.	high and medium impact BCS and associated SCI, more than five percent but less than or equal to 10 percent high or medium BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than five but less than or equal to 10 high or medium BCS or associated SCI have not been identified.	high and medium impact BCS and associated SCI, more than 10 percent but less than or equal to 15 percent high or medium BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 10 but less than or equal to 15 high or medium BCS or associated SCI have not been identified.	associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 15 high or medium impact BCS or associated SCI have not been identified.
R2.	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months but less than or equal to 16 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part 2.2)	16 calendar months but less than or equal to 17 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part 2.2)	17 calendar months but less than or equal to 18 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part 2.2)	18 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part 2.2)

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Virtualization Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	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 Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata

Version	Date	Action	Change Tracking
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization conforming changes	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating

Each BCS used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating

Each BCS, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are those shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7~~6~~

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the BES. Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises 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 ~~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-002-7~~6~~:

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~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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 Date:** See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-002-6.~~

~~6. **Background:** This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements 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 and the criteria in Attachment 1 of CIP-002 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.~~

~~**BES Cyber Systems**~~

~~The CIP Cyber Security Standards use the “BES Cyber System” term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES~~

~~Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.~~

~~**Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems**~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

- ~~**Electronic Access Control or Monitoring Systems (“EACMS”) –** Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
- ~~**Physical Access Control Systems (“PACS”) –** Examples include: authentication servers, card systems, and badge control systems.~~
- ~~**Protected Cyber Assets (“PCA”) –** Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber System~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber System~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~ BCS or SCI that hosts any portion of a low impact BCS is not required).

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.5. Identify associated SCI that hosts any portion of the medium impact ~~BES Cyber System~~BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1, and 1.2, 1.4 and 1.5~~.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2. Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

~~**1.4. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Systems~~BCS, and associated SCI, five percent or fewer of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, five or fewer identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber Systems~~BCS and associated SCI, more than five but less than or equal to 10 identified ~~BES Cyber~~	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber Assets~~BCS and associated SCI, more than 10 but less than or equal to 15 identified ~~BES Cyber~~	~~Systems~~BCS and associated SCI, more than 15 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, and associated SCI, five percent or fewer high or medium ~~BES Cyber Systems~~BCS or associated SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, or associated SCI, five or fewer high or medium ~~BES Cyber Systems~~BCS or associated SCI, have not been identified.	~~Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	~~Assets~~ BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 high or medium impact ~~BES Cyber Systems~~BCS or associated SCI have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber Systems~~BCS and associated SCI, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified.	~~Cyber Systems~~BCS and associated SCI, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified.	
R2.	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity did not complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan ~~for CIP-002-76~~.”
- ~~See Appendix 1. The Interpretation in Appendix 1 was developed under a prior version of the Reliability Standard, CIP-002-5.1, and is being carried forward to subsequent versions.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	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 Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata

Version	Date	Action	Change Tracking
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization conforming changes	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High Impact Rating**

   Each ~~BES Cyber System~~BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium Impact Rating**

   Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~ each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are those shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Remedial Action Scheme (~~RAS~~)~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~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. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified 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. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-6~~

~~CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:~~

- ~~Dynamic Response to BES conditions~~

- ~~Balancing Load and Generation~~
- ~~Controlling Frequency (Real Power)~~
- ~~Controlling Voltage (Reactive Power)~~
- ~~Managing Constraints~~
- ~~Monitoring & Control~~
- ~~Restoration of BES~~
- ~~Situational Awareness~~
- ~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~Entity Registration~~	~~RC~~	~~BA~~	~~TOP~~	~~TO~~	~~DP~~	~~GOP~~	~~GO~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~
- ~~Non-spinning reserve (contingency reserve)~~

  - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
  - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
  - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
  - ~~Software to calculate unit adjustments (BA)~~
  - ~~Transmit adjustments to individual units (GOP)~~
  - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
  - ~~Frequency source, schedule (BA)~~
  - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
  - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
  - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
  - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
  - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~

- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and~~

~~operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~
~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~
~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Attachment 1~~
~~Overall Application~~
~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

~~When the drafting team uses the term "Facilities," there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may~~

~~be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~

~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~

~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.~~

~~*Generation*~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

  ~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units~~

~~designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~***Transmission***~~

~~*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical*~~

~~*borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.*~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

  ~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~

  - ~~Excluded radial facilities that would only provide support for single generation facilities.~~

  - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

  ~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~

2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted~~

~~that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. 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.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.~~

  ~~The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.~~

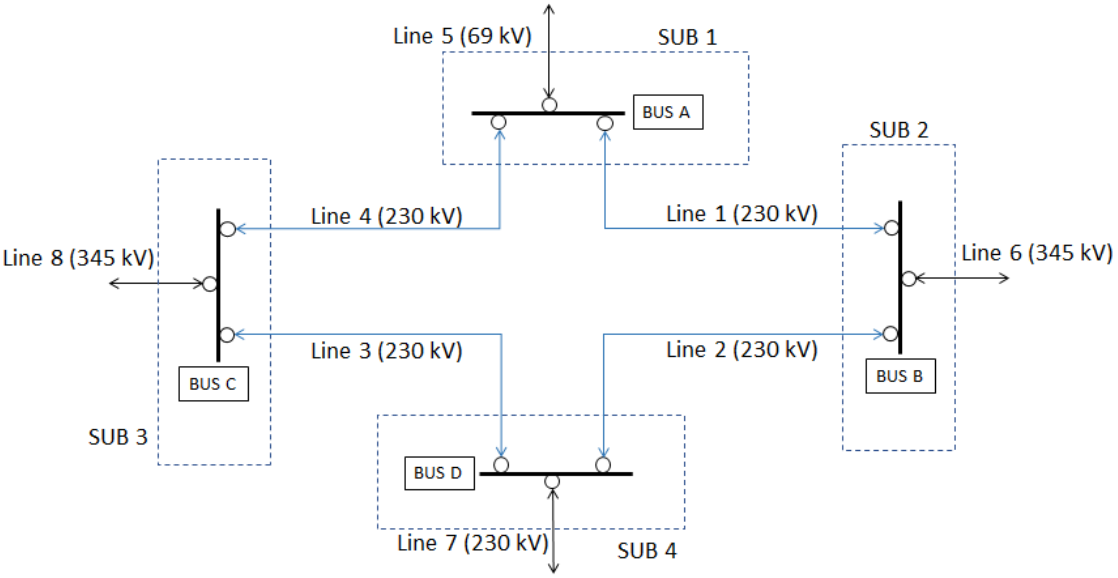
  ~~In the terms of applicable BES Transmission Lines, the following should be considered:~~

  - ~~All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).~~

- ~~All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity's Control Center, including associated data center(s).~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.12 Examples:~~

~~In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 1~~

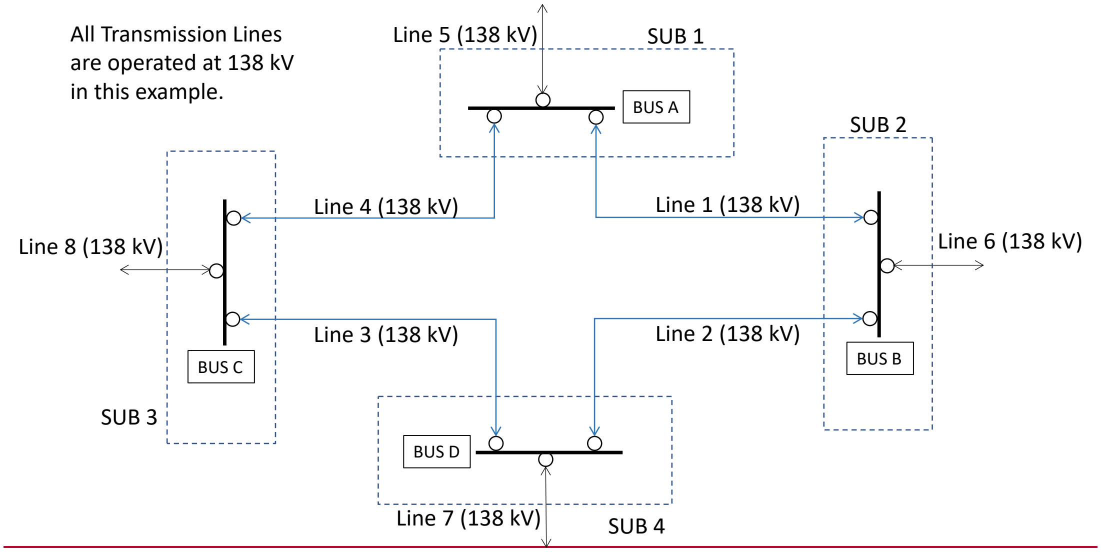
~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~Line 5~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~None~~	~~0~~
~~200 kV to 299 kV~~	~~700~~	~~Line 1, Line 2, Line 3, Line 4, Line 7~~	~~3500~~
~~300 kV to 499 kV~~	~~1300~~	~~Line 6, Line 8~~	~~2600~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~700+700+700+700+700+1300+1300 = 6100~~

~~In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 2~~

~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~None~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8~~	~~2000~~
~~200 kV to 299 kV~~	~~700~~	~~None~~	~~0~~
~~300 kV to 499 kV~~	~~1300~~	~~None~~	~~0~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~250+250+250+250+250+250+250+250= 2000~~

- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

  ~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

  ~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection~~

~~point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

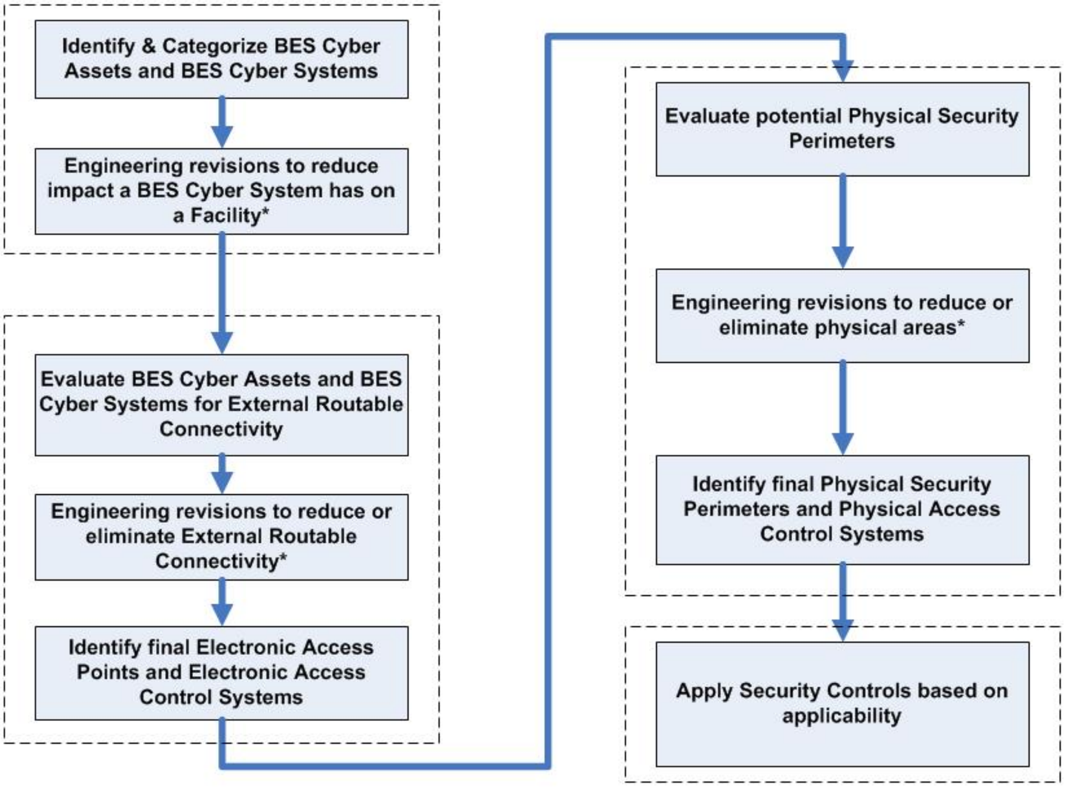
~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~

~~Appendix 1 – Interpretation~~

Overview (Generation Facility)


Identify & Categorize BES Cyber Assets and BES Cyber Systems
Engineering revisions to reduce impact a BES Cyber System has on a Facility*
Evaluate BES Cyber Assets and BES Cyber Systems for External Routable Connectivity
Engineering revisions to reduce or eliminate External Routable Connectivity*
Identify final Electronic Access Points and Electronic Access Control Systems
Evaluate potential Physical Security Perimeters
Engineering revisions to reduce or eliminate physical areas*
Identify final Physical Security Perimeters and Physical Access Control Systems
Apply Security Controls based on applicability

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~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 R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~

~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~2. Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

~~2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

~~Questions~~

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

1. ~~Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
2. ~~Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
3. ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of~~

~~the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~

> ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~**Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?**~~

~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

> ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.~~

~~**Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?**~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21, 2021–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

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

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:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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.

5. **Effective Dates:** See “Project 2016-02 Virtualization Implementation Plan.”

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 BCS and associated SCI, 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 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 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 BCS and associated SCI, 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; and

1.2.6. 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 BCS shall implement one or more documented cyber security plan(s) for its low impact BCS and their associated SCI 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 BCS or their associated SCI 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 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address one of the nine topics required by Requirement R1. (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 BCS and associated SCI as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) 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 BCS and associated SCI as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address three of the nine topics required by Requirement R1. (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 BCS and associated SCI as required by Requirement R1 within 17 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address four or more of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.1) 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 BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R1 Part 1.1) 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 and associated SCI as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part 1.1) 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 BCS and associated SCI 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	(Requirement R1 Part 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 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 BCS and associated SCI as

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI 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. (Requirement 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	complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI 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. (Requirement R 1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for	calendar months of the previous review. (Requirement 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 BCS and associated SCI 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 Part 1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1. (Requirement 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 BCS and associated SCI as required by Requirement R1 by

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			containing low impact BCS and associated SCI 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. (Requirement R1 Part 1.2)	its assets identified in CIP-002 containing low impact BCS and associated SCI 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. (Requirement R1 Part 1.2)		the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to document cyber security awareness according	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to reinforce cyber security practices at least	The Responsible Entity documented the physical access controls for its assets containing low impact BCS and associated SCI but failed to implement the physical security controls according to Requirement R2,	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS and associated SCI according to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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 security plan(s) for its assets containing low impact BCS and associated SCI but failed to document	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 BCS and associated SCI but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security	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 BCS and associated SCI 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 documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for assets containing low impact	Requirement R2, Attachment 1. (Requirement R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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 BCS and associated SCI but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1,	plan(s) for its assets containing low impact BCS and associated SCI 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 BCS, per Cyber Asset capability according to Requirement R2, Attachment 1,	BCS and associated SCI 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	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 BCS and associated SCI, 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	The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				its cyber security plan(s) for its assets containing low impact BCS and associated SCI 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 TCA and Removable	Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Media, but failed to document mitigation for the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	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 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	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 not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the change. (Requirement R3)	50 calendar days of the change. (Requirement R3)		not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	**Operations Planning**	**Lower**	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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

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.

Version	Date	Action	Change Tracking
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.
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 BCS.
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	

Version	Date	Action	Change Tracking
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	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI

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 BCS ratings can utilize policies, procedures, and processes for their high or medium impact 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 BCS within the asset, (2) the asset or the locations of the of the SCI hosting low impact BES Cyber Assets within the asset, and (3) 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 BCS or its associated SCI 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 a low impact BCS and a system(s) outside the asset containing low impact BCS;

ii. between a SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;

iii. using a routable protocol when entering or leaving the asset containing the low impact BCS or their associated SCI; and

iv. 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).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or their associated SCI, per Cyber Asset or VCA 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. 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 BCS or its associated SCI, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For 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 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 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 TCA to a low impact BCS or its associated SCI (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 method(s) to mitigate the 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 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 BCS or its associated SCI; 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 BCS or its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI

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 BCS or their associated SCI within the asset; and
  b. The Cyber Asset(s), VCA, or SCI 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 BCS, routable communication between a low impact BCS and systems outside the asset 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 used for time-sensitive protection or control functions between intelligent electronic devices. 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 BCS and systems outside the asset containing low impact BCS 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 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. 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 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 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 TCA managed by a party other than the Responsible Entity. If a 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 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 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.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21, 2021–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-9~~8~~

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~~8~~:

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)~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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 Virtualization Implementation Plan." ~~for Project CIP-003-8~~

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

~~Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~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 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.~~

~~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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. 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.~~

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 and associated SCI, 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 and associated SCI, 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; and

1.2.6. 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 ~~BES Cyber Systems~~BCS and their associated SCI 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 associated SCI ~~BES Cyber Assets~~ 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 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.

~~**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 #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact~~ BES Cyber Systems~~ BCS and associated SCI but did not address one of the nine topics required by Requirement R1. (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	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) 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	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address three of the nine topics required by Requirement R1. (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 and associated SCI as required by Requirement	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address four or more of the nine topics required by Requirement R1. (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 and associated SCI as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			and associated SCI 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. (Requirement R1 Part 1.1) 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 and associated SCI as required by Requirement R1 by the CIP Senior	and associated SCI 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. (Requirement R1 Part ~~R~~1.1) 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 and associated SCI as required by Requirement R1 by the CIP Senior	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part ~~R~~1.1) 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 and associated SCI 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)	required by Requirement R1. (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 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 ~~R~~Part 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 and associated SCI but did not address one of the six topics required by Requirement R1. (Requirement R1 ~~R~~Part 1.2)	Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 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 and associated SCI but did not address two of the six topics required by Requirement R1. (Requirement R1 Part ~~R~~1.2)	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 and associated SCI, but did not address three of the six topics required by Requirement R1. (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 and associated SCI as required by Requirement R1 within 17 calendar	medium impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 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 and associated SCI but did not address four or more of the six topics required by Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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 and associated SCI 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. (Requirement R1 ~~R~~Part 1.2) OR The Responsible Entity did not complete its	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 and associated SCI 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. (Requirement R 1 Part ~~R~~1.2) OR The Responsible Entity did not complete its	months but did complete this review in less than or equal to 18 calendar months of the previous review. (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 and associated SCI 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 Part ~~R~~1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1. (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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI 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. (Requirement R1 Part ~~R~~1.2)	approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI 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. (Requirement R1 Part ~~R~~1.2)	(Requirement R1 Part ~~R~~1.2)	in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented the physical access controls for its assets containing low impact ~~BES Cyber~~	The Responsible Entity failed to document and implement one or more cyber security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact ~~BES Cyber Systems~~ BCS and associated SCI 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	impact ~~BES Cyber Systems~~ BCS and associated SCI 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~~ BCS and associated SCI but failed to document physical security controls according to Requirement R2, Attachment 1,	~~Systems~~ BCS and associated SCI 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~~ BCS and associated SCI but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR	plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI according to Requirement R2, Attachment 1. (Requirement R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI 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~~ BCS and associated SCI	Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI 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	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~~ BCS and associated SCI 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	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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 TCA and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to	Dial-up Connectivity that provides access to low impact ~~BES Cyber System(s)~~BCS, 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 Cyber Systems~~ BCS and associated SCI, but failed to include the process for identification, classification, and response to Cyber Security Incidents	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 TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	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~~ BCS and associated SCI 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	the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~ BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				document mitigation for the introduction of malicious code for TCA 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 TCA and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified	The Responsible Entity has identified	The Responsible Entity has identified by name a	The Responsible Entity has not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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)	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)	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)	identified, 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)
R4	Operations Planning	Lower	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	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	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	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)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (Requirement R4)	change in less than 50 calendar days of the change. (Requirement R4)	change. (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

~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”

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.

Version	Date	Action	Change Tracking
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.
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~~BCS.
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	

Version	Date	Action	Change Tracking
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	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES Cyber Systems~~BCS or their associated SCI

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, (2) the asset or the locations of the of the SCI hosting low impact BES Cyber Assets within the asset, and (3~~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)~~ BCS or its associated SCI 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 a low impact ~~BES Cyber System(s)~~BCS and a ~~Cyber Asset(s)~~system(s) outside the asset containing low impact ~~BES Cyber System(s)~~BCS;

~~i.~~ii. between a SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;

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

~~iii.~~iv. 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).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s)~~ BCS or their associated SCI, per Cyber Asset or VCA 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 or its associated SCI, 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~~TCA to a low impact ~~BES Cyber System~~ BCS or its associated SCI (per ~~Transient Cyber Asset~~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 method(s) to mitigate the 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 its associated SCI; 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 its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES Cyber Systems~~BCS or their associated SCI

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 or their associated SCI within the asset; and

  b. The Cyber Asset(s), VCA, or SCI 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~~BCS, routable communication between a low impact ~~BES Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset 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 used for time-sensitive protection or control functions between intelligent electronic devices. 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)~~BCS and ~~a Cyber Asset(s)~~systems outside the asset containing low impact ~~BES Cyber System(s)~~BCS 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.

~~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. 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:~~

~~In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.~~

~~If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.~~

~~Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.~~

~~Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC’s cyber security Reliability Standards will not be considered candidates for potential violations~~

~~although they will help demonstrate the organization’s internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

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

~~Organization position on acceptable background investigations~~

~~Identification of possible disciplinary action for violating this policy~~

~~Account management~~

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

~~Organization stance on use of wireless networks~~

~~Identification of acceptable authentication methods~~

~~Identification of trusted and untrusted resources~~

~~Monitoring and logging of ingress and egress at Electronic Access Points~~

~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~

~~Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~

~~Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access~~

~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls~~

~~Physical security of BES Cyber Systems (CIP-006)~~

~~Strategy for protecting Cyber Assets from unauthorized physical access~~

~~Acceptable physical access control methods~~

~~Monitoring and logging of physical ingress~~

~~System security management (CIP-007)~~

~~Strategies for system hardening~~

~~Acceptable methods of authentication and access control~~

~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~

~~Monitoring and logging of BES Cyber Systems~~

~~Incident reporting and response planning (CIP-008)~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

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

~~Availability of spare components~~

~~Availability of system backups~~

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

~~Initiation of change requests~~

~~Approval of changes~~

~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

~~Information access control methods~~

~~Notification of unauthorized information disclosure~~

~~Information access on a need-to-know basis~~

~~1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~

~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

~~Method(s) for delivery of security awareness~~

~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

~~Process(es) to declare a CIP Exceptional Circumstance~~

~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~Requirement R2:~~

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

~~Requirement R2, Attachment 1~~

~~As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.~~

~~Guidance for each of the subject matter areas of Attachment 1 is provided below.~~

~~Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness~~

~~The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.~~

~~Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 2 – Physical Security Controls~~

~~The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.~~

~~The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with~~

~~locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

~~Requirement R2, Attachment 1, Section 3 – Electronic Access Controls~~

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

~~The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.~~

~~Electronic Access Control Exclusion~~

~~In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access 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. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~

~~Considerations for Determining Routable Protocol Communications~~

~~To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.~~

~~When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles~~

~~away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

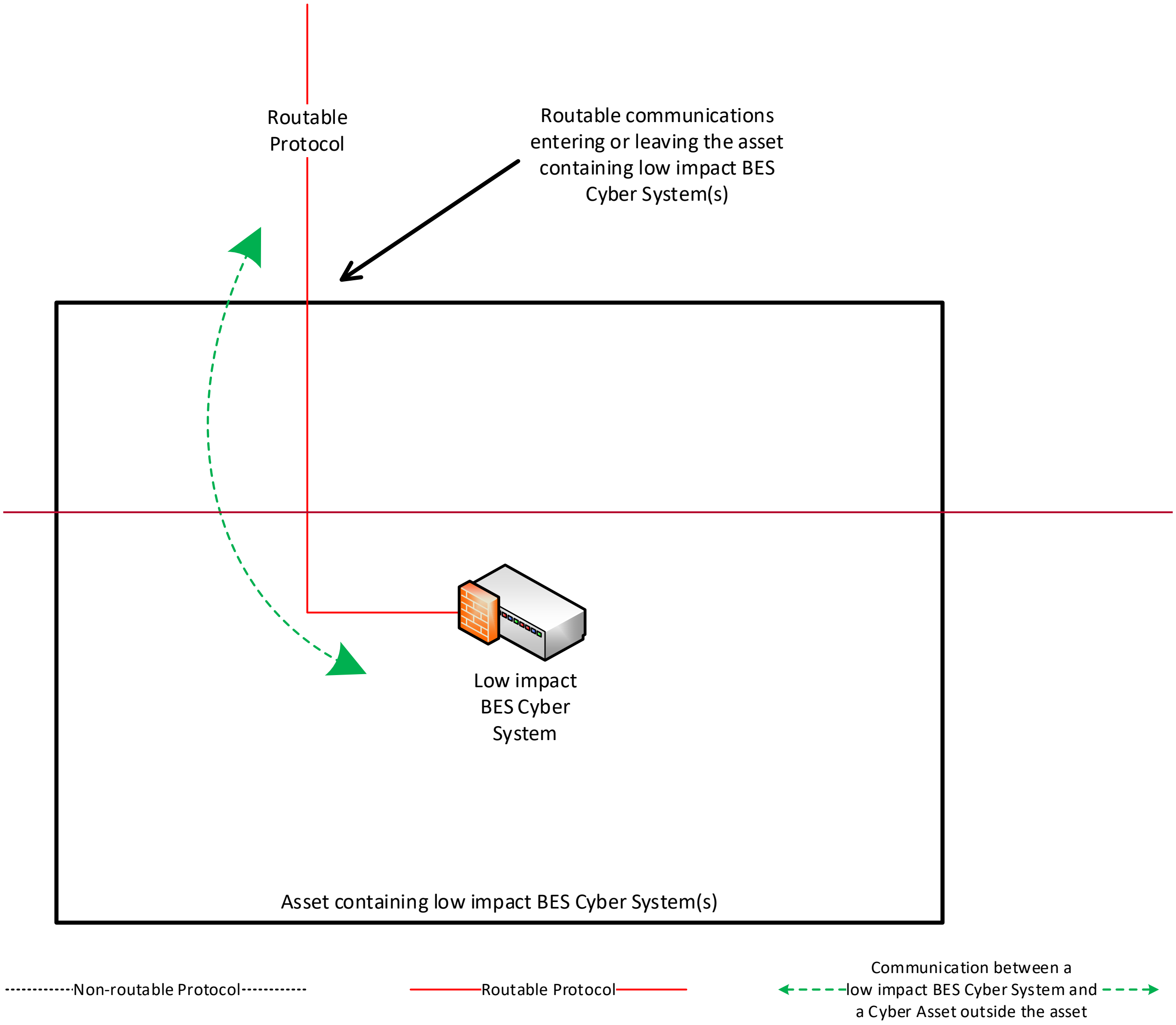
~~**NOTE:**~~

~~This is not an exhaustive list of applicable concepts.~~

~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

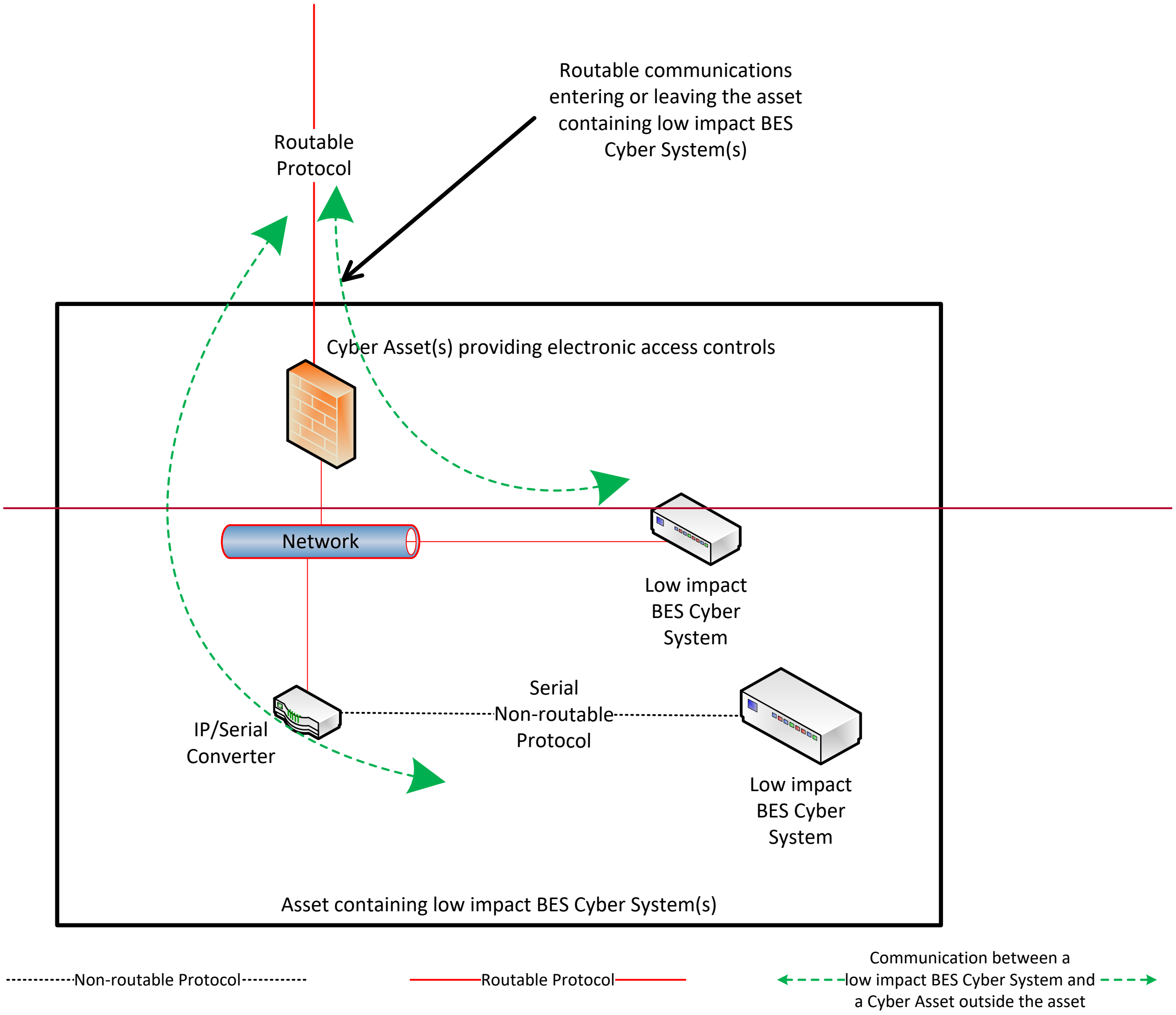
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~


Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 1~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

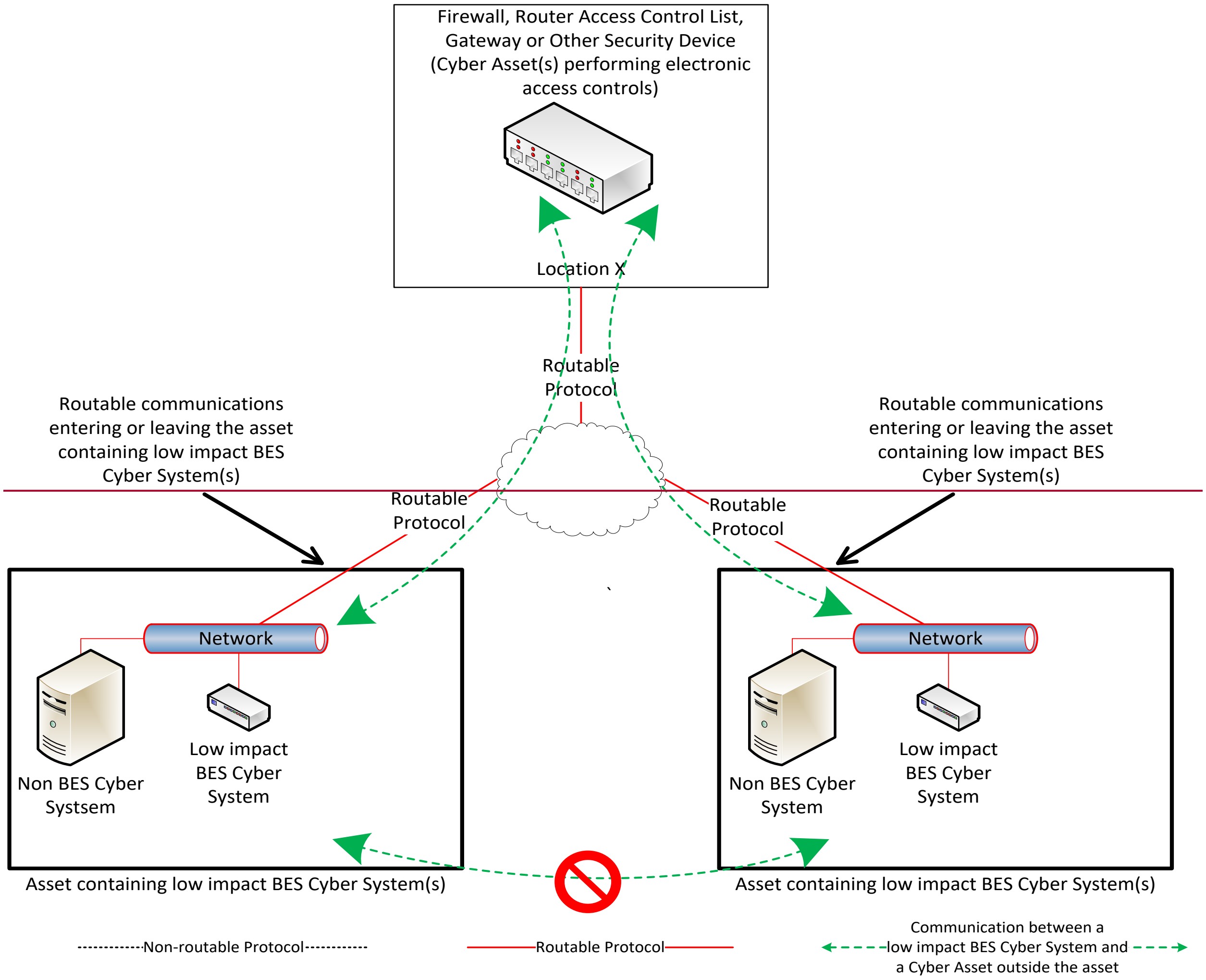
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~


Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
Cyber Asset(s) providing electronic access controls
Network
Low impact BES Cyber System
Serial Non-routable Protocol
IP/Serial Converter
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 2~~

~~Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

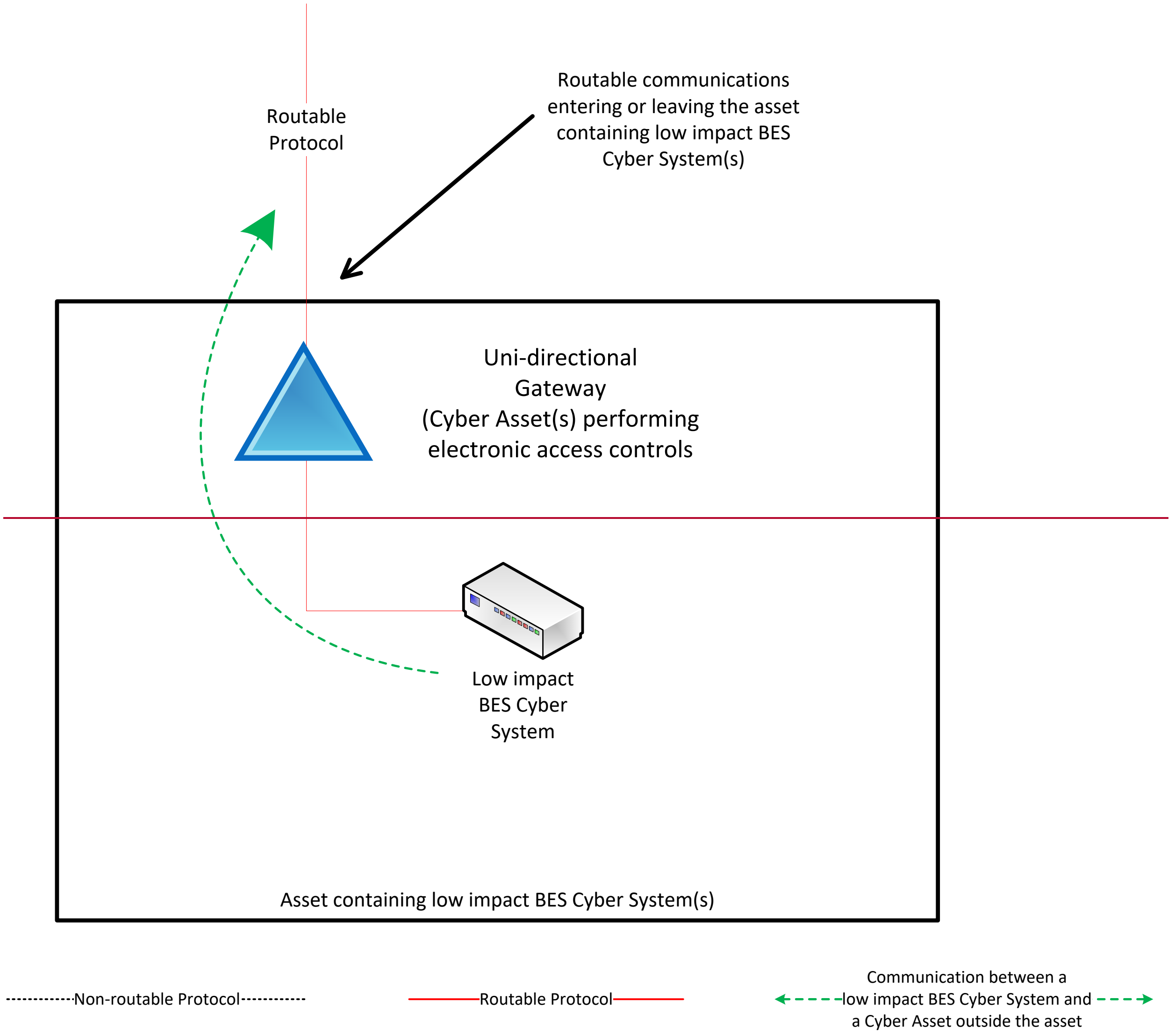
~~The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~


Firewall, Router Access Control List, Gateway or Other Security Device (Cyber Asset(s) performing electronic access controls)
Location X
Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
Routable Protocol
Network
Non BES Cyber Systsem
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Network
Non BES Cyber System
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
------------Non-routable Protocol-----------
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 3~~

~~Reference Model 4 – Uni-directional Gateway~~

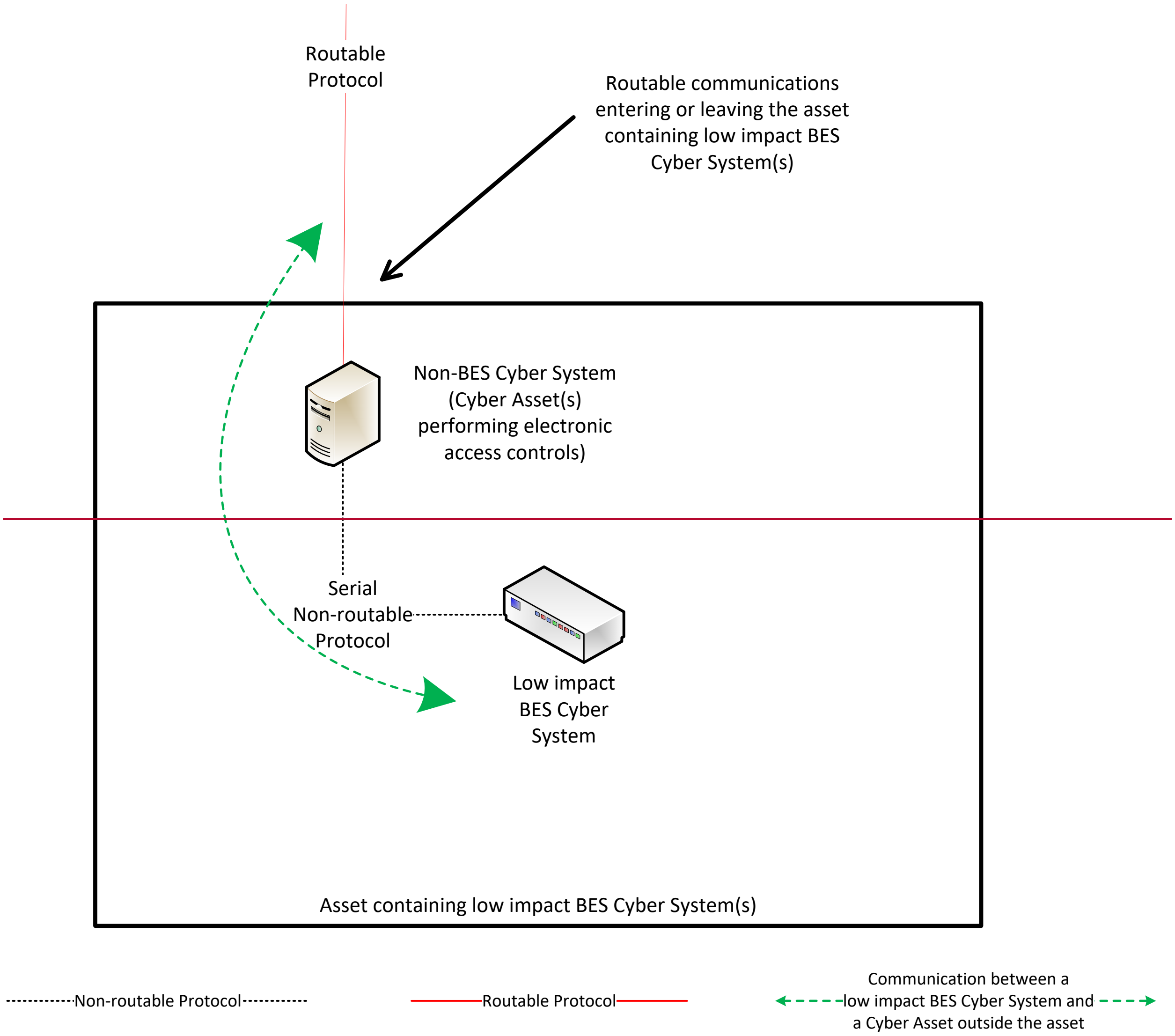
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~


Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Uni-directional Gateway (Cyber Asset(s) performing electronic access controls
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 4~~

~~Reference Model 5 – User Authentication~~

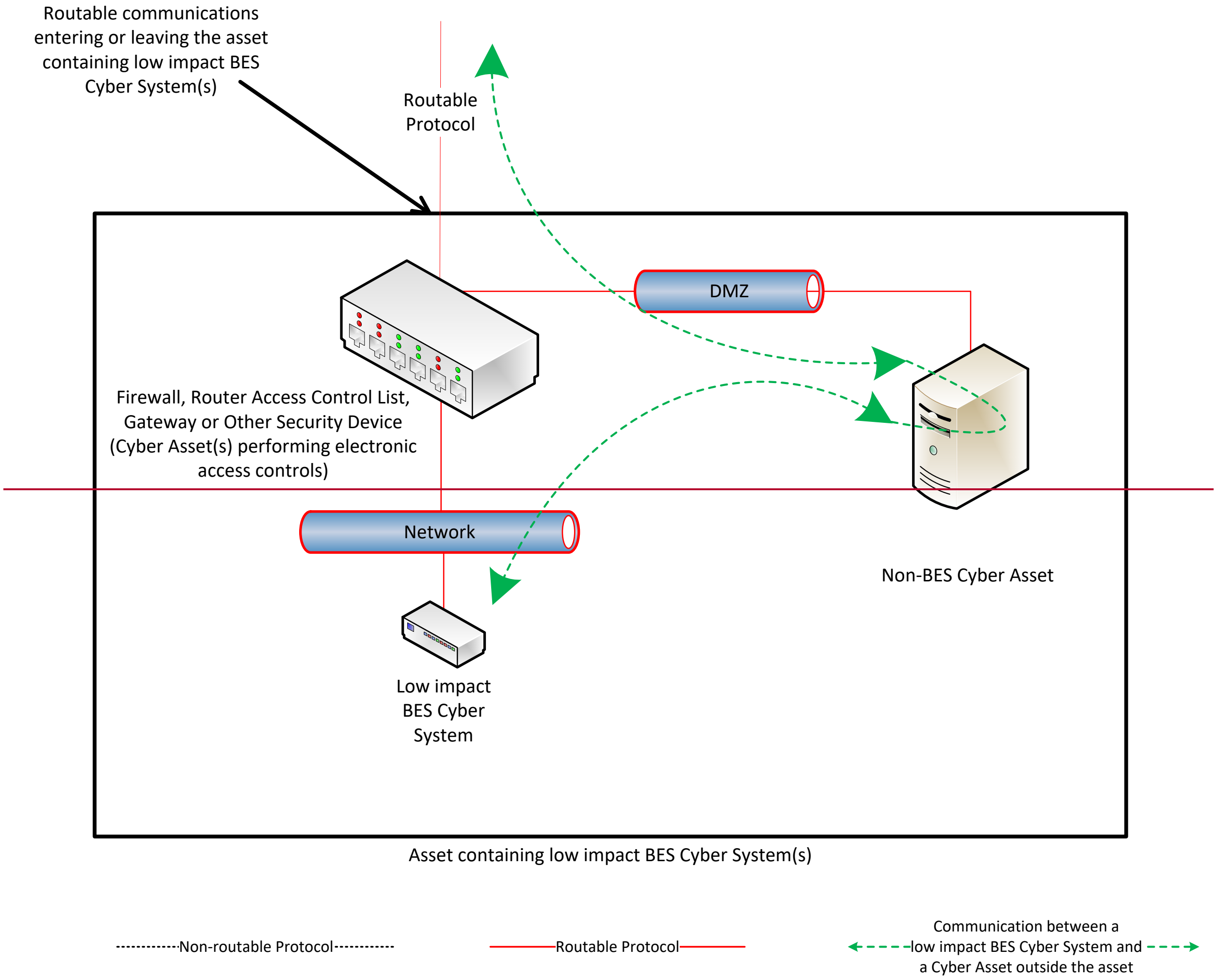
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~


Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Non-BES Cyber System (Cyber Asset(s) performing electronic access controls)
Serial Non-routable Protocol
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~*Reference Model 5*~~

~~Reference Model 6 – Indirect Access~~

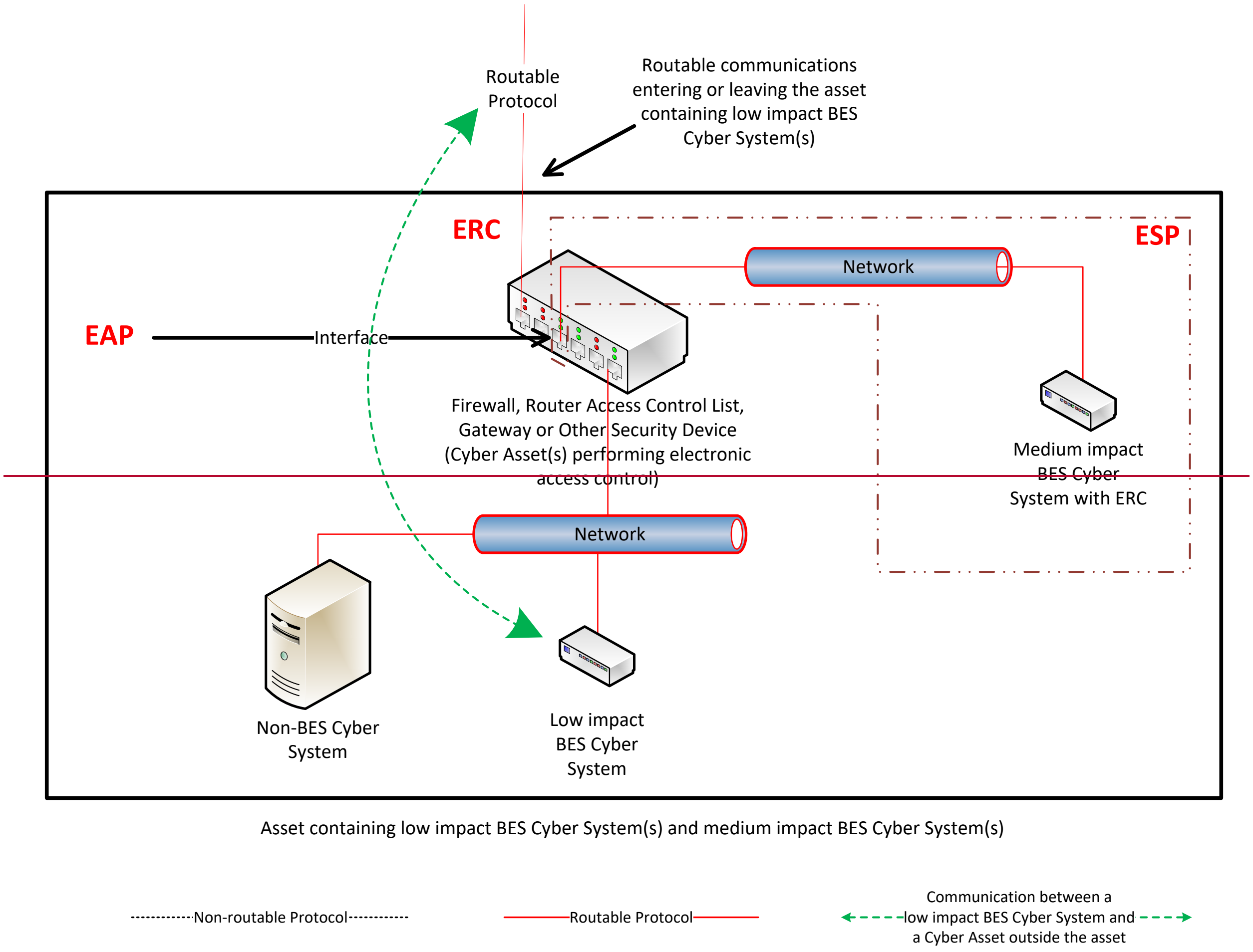
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~


Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device (Cyber Asset(s) performing electronic access controls)
Network
Non-BES Cyber Asset
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 6~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~


Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
ERC
ESP
Network
EAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device (Cyber Asset(s) performing electronic access control)
Medium impact BES Cyber System with ERC
Network
Non-BES Cyber System
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s) and medium impact BES Cyber System(s)
------------Non-routable Protocol-----------
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 7~~

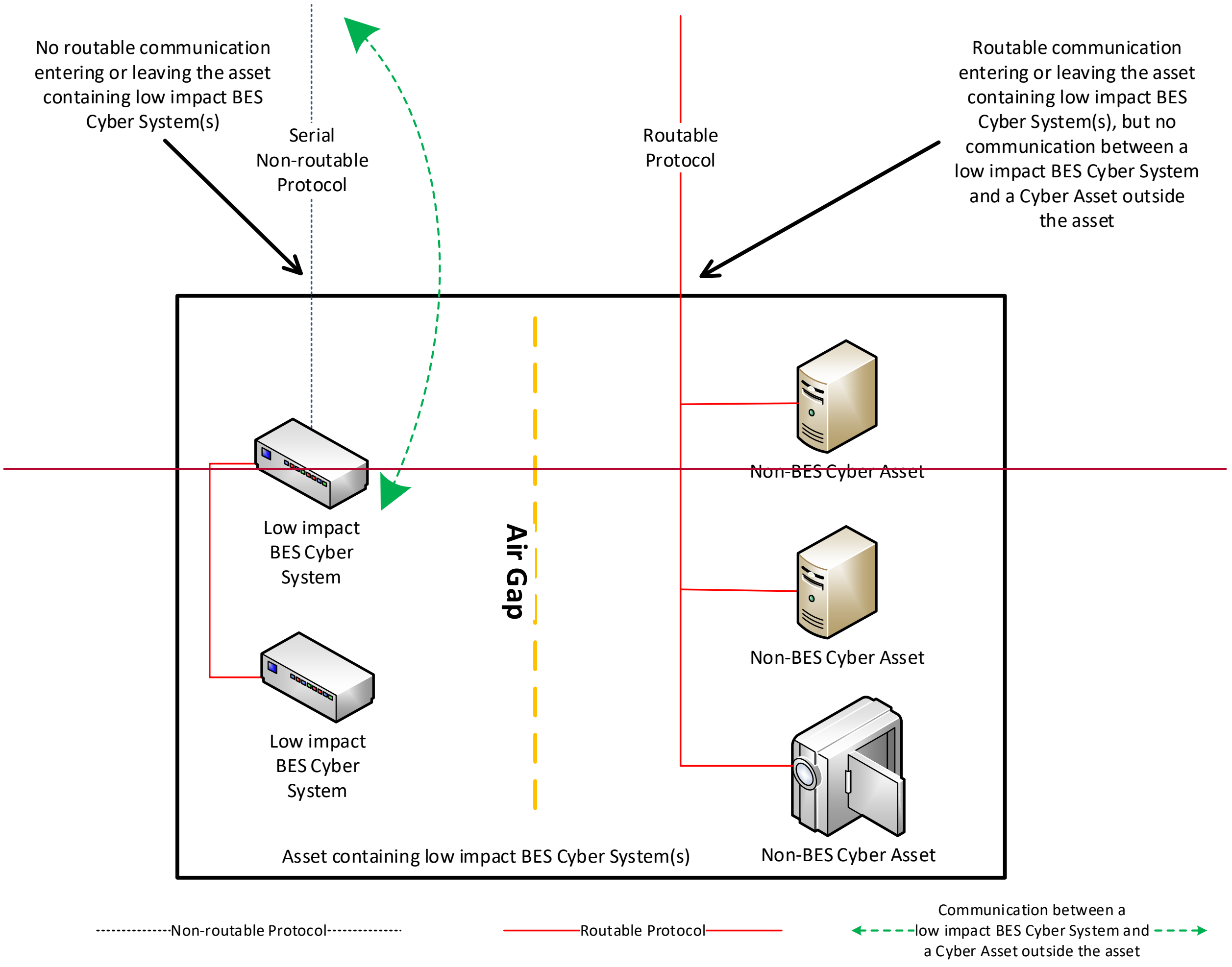
~~Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

~~The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

~~The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

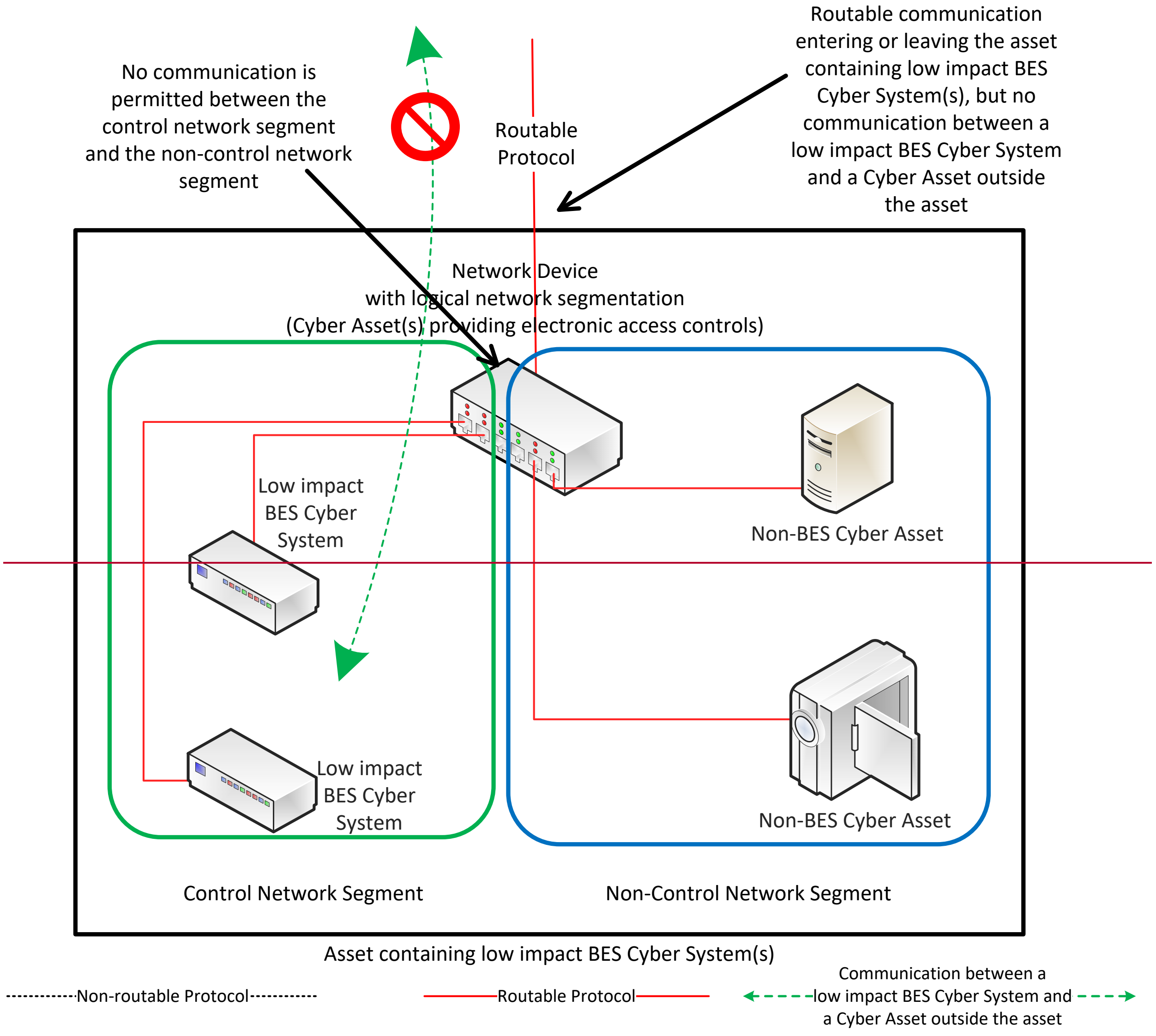
~~The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~


No routable communication entering or leaving the asset containing low impact BES Cyber System(s)
Serial Non-routable Protocol
Routable Protocol
Routable communication entering or leaving the asset containing low impact BES Cyber System(s), but no communication between a low impact BES Cyber System and a Cyber Asset outside the asset
Non-BES Cyber Asset
Low impact BES Cyber System
Air Gap
Non-BES Cyber Asset
Low impact BES Cyber System
Non-BES Cyber Asset
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 8~~

~~Reference Model 9 – Logical Isolation - No Electronic Access Controls Required~~

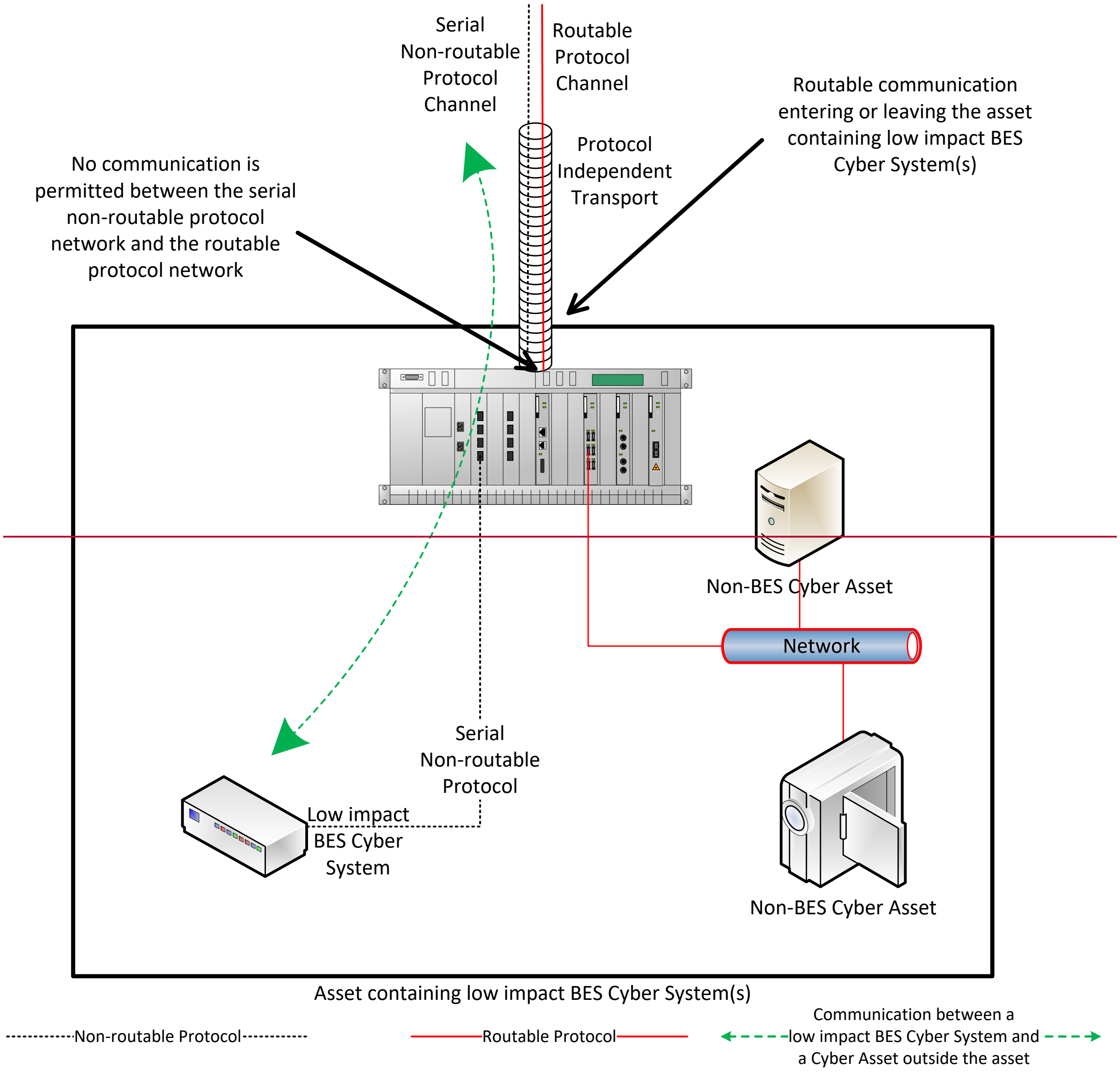
~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~


No communication is permitted between the control network segment and the non-control network segment
Routable Protocol
Routable communication entering or leaving the asset containing low impact BES Cyber System(s), but no communication between a low impact BES Cyber System and a Cyber Asset outside the asset
Network Device with logical network segmentation (Cyber Asset(s) providing electronic access controls)
Low impact BES Cyber System
Non-BES Cyber Asset
Low impact BES Cyber System
Non-BES Cyber Asset
Control Network Segment
Non-Control Network Segment
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 9~~

~~Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~


Serial
Non-routable
Protocol
Channel
Routable
Protocol
Channel
Routable communication entering or leaving the asset containing low impact BES Cyber System(s)
Protocol
Independent
Transport
No communication is permitted between the serial non-routable protocol network and the routable protocol network
Non-BES Cyber Asset
Network
Serial
Non-routable
Protocol
Low impact
BES Cyber
System
Non-BES Cyber Asset
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

~~Reference Model 10~~

~~Dial-up Connectivity~~

~~Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.~~

~~Insufficient Access Controls~~

~~Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:~~

~~An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.~~

~~A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.~~

~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.~~

~~Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response~~

~~The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.~~

~~Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.~~

~~The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.~~

~~For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets.~~

~~Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

~~Diagnostic test equipment;~~

~~Equipment used for BES Cyber System maintenance; or~~

~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

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

~~Malicious Code Risk Mitigation~~

~~The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~Per Transient Cyber Asset Capability~~

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

~~Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~**Section 5.1:** Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~

~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~

~~When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

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

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

~~**Section 5.2.1:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~

~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~**Section 5.2.2:** The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

~~Requirement R2, Attachment 1, Section 5.3 – Removable Media~~

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

~~**Section 5.3:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in~~

~~conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.~~

~~**Requirement R3:**~~

~~The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.~~

~~**Requirement R4:**~~

~~As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.~~

~~The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

~~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:~~

~~One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~Rationale for Requirement R2:~~

~~In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

~~Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (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)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~Rationale for Section 5 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for~~

~~responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-7

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BCS.

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-004-7:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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 BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated SCI Medium Impact BCS and their associated SCI	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BCS or SCI.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

2.1	High Impact BCS and their associated:
	1. Electronic Access Control or Monitoring System (EACMS); and
	2. Physical Access Control Systems (PACS)
	Medium Impact BCS, with External Routable Connectivity (ERC) or Interactive Remote Access (IRA), and their associated:
	1. EACMS; and
	2. PACS
	SCI hosting High Impact BCS or their associated:
	• EACMS; or
	• PACS
	SCI, with ERC or IRA, hosting Medium Impact BCS or their associated:
	• EACMS; or
	• PACS
		Training content on:
		2.1.1. Cyber security policies;
		2.1.2. Physical access controls;
		2.1.3. Electronic access controls;
		2.1.4. The visitor control program;
		2.1.5. Handling of BES Cyber System Information (BCSI) and its storage;
		2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
		2.1.7. Recovery plans for BCS and SCI;
		2.1.8. Response to Cyber Security Incidents; and
		2.1.9. Cyber security risks associated with a BCS and SCI's electronic interconnectivity and interoperability with other Cyber Assets and VCA, including Transient Cyber Assets, and with Removable Media.
			Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, VCA or SCI, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BCS or their associated SCI that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven-year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven-year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BCSI.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BCSI.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS: and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated EACMS or PACS. SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	A process to initiate removal of an individual’s ability for unescorted physical access and IRA upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For termination actions, revoke the individual's access to the designated storage locations for BCSI, whether physical or electronic (unless already revoked according to Requirement R5 Part 5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any applicable systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated: • EACMS.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

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 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-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	unescorted physical access but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	(Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for	or more individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	3.2.1 and 3.2.2 for one individual. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BCSI is located. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BCSI	groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	storage locations, privileges were incorrect or unnecessary. Requirement R4 Part (4.4)		necessary within 15 calendar months of the previous verification but for more than 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI, but for one individual, did not do so by the end of the next calendar day following the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (Requirement R5 Part 5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BCSI storage locations. (Requirement R5 Part R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	effective date and time of the termination action. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more process(es) to	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI but, for two individuals, did not do so by the end of the next calendar	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	hours of the termination action but did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or	day following the effective date and time of the termination action. (Requirement R5 Part 5.3)		

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 Virtualization Implementation Plan."

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.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
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	2/12/15	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 BCS.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-7 ~~6~~

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting ~~BES Cyber Systems~~BCS.

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-004-7~~6~~:

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~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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.

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

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:** See "Project 2016-02 Virtualization implementation Plan." ~~for CIP-004-6~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~ BCS and their associated SCI Medium Impact ~~BES Cyber Systems~~ BCS and their associated SCI	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~BCS or SCI.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures

2.1	High Impact ~~BES Cyber Systems~~ BCS and their associated:
	1. Electronic Access Control or Monitoring System (EACMS); and
	2. Physical Access Control Systems (PACS)
	Medium Impact ~~BES Cyber Systems~~BCS, with External Routable Connectivity (ERC) or Interactive Remote Access (IRA), and their associated:
	1. EACMS; and
	2. PACS
	SCI hosting High Impact BCS or their associated:
	• EACMS; or
	• PACS
	SCI, with ERC or IRA, hosting Medium Impact BCS or their associated:
	• EACMS; or
	• PACS
		Training content on:
		2.1.1. Cyber security policies;
		2.1.2. Physical access controls;
		2.1.3. Electronic access controls;
		2.1.4. The visitor control program;
		2.1.5. Handling of BES Cyber System Information (BCSI) and its storage;
		2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
		2.1.7. Recovery plans for ~~BES Cyber Systems~~ BCS and SCI;
		2.1.8. Response to Cyber Security Incidents; and
		2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~ BCS and SCI's electronic interconnectivity and interoperability with other Cyber Assets and VCA, including Transient Cyber Assets, and with Removable Media.
			Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, VCA or SCI, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ BCS or their associated SCI that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-~~-~~years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven-~~-~~year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven-~~-~~year criminal history records check.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.4	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~ IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC- or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7~~6~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for ~~BES Cyber System Information~~BCSI.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for ~~BES Cyber System Information~~BCSI.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS: and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: - Dated ~~-~~documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or - Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7~~6~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Verify at least once every 15 calendar months that access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for ~~BES Cyber System Iinformation~~BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated EACMS or PACS. SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	A process to initiate removal of an individual's ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For termination actions, revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic (unless already revoked according to Requirement R5 Part 5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing ~~BES Cyber System Information~~BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any ~~individual~~ applicable ~~BES Cyber Assets~~systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated: • EACMS.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

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 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.

~~1.3. Compliance Monitoring and Assessment Processes:~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	unescorted physical access but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	(Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for	or more individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	3.2.1 and 3.2.2 for one individual. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where ~~BES Cyber System~~

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber~~applicable ~~S~~systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its ~~BES Cyber S~~applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than	groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber S~~applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	~~Information~~BCSI is located. (Requirement R4 Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber~~applicable ~~S~~systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	(or equal to) 10% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. Requirement R4 Part (4.4)		The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or ~~BES Cyber System Information~~BCSI storage locations. (Requirement R5 Part R5) OR

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Information~~BCSI, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4)	24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more	initiate those removals for two individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document	process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	~~Information~~BCSI but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~See "Project 2016-02 Virtualization Implementation Plan."

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.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
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	2/12/15	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~~BCS.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Logical Isolation

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication to reduce the likelihood of misoperations or instability in the BES.

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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 BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Logical Isolation*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); 2. Physical Access Control Systems (PACS) hosted on SCI; and 3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact BCS connected to a network via a routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI	Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration); that enforces electronic access control and logical isolation and documents the business need.

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS	Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS connected to a network via routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: • confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other nonprogrammable communication components, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption).

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated: • PCS; • PACS; or • EACMS	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS at Control Centers and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PCA; • PACS, or • EACMS	Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: - PCA Medium Impact BCS with Interactive Remote Access (IRA) and their associated: - PCA SCI with IRA hosting High or Medium Impact BCS or their associated: - PCA; - PACS; or - EACMS Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: - PCA; - PACS; or - EACMS	Ensure that IRA is through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access applicable systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA	An example of evidence may include, but is not limited to, architecture documents detailing where

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		between the client and the Intermediate System.	confidentiality and integrity controls initiate and terminate.
2.3	Intermediate Systems used to access applicable systems of Part 2.1	Require multi-factor authentication to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including IRA and system-to-system remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Intermediate Systems used to access applicable systems of Part 2.1	Implement for applicable systems as follows: **2.6.1.** Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	Examples of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with External	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Routable Connectivity (ERC) SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS		remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Logical Isolation*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. (Requirement R1 Part 1.1) OR The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				capability (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not implement a method to protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other nonprogrammable communication components (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the applicable systems. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable	The Responsible Entity did not implement processes for two of the applicable	The Responsible Entity did not implement processes for three of the applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS, SCI, and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS, SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking

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

6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System -Logical Isolation~~Electronic Security Perimeter(s)~~

2. **Number:** CIP-005-8~~7~~

3. **Purpose:** To ~~manage electronic access to~~protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication~~.by specifying a controlled Electronic Security Perimeter~~ to reduce the likelihood of misoperations or instability in the BES. ~~in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.~~

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8~~7~~:

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~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber ~~S~~systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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.

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

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03.~~

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

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

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

~~documented processes, but it must address the applicable requirements in the table.~~

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

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

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

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

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

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

~~"Applicable Systems" Columns in Tables:~~

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

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

~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~

~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

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

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); ~~1.~~2. Physical Access Control Systems (PACS) hosted on SCI; and ~~2.~~3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. PCA; ~~1.~~2. PACS hosted on SCI; and ~~2.~~3. EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP~~ Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	~~An e~~Examples of evidence may include, but is not limited to, ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP~~documentation that includes the configuration of systems ~~that enforce electronic access control and logical isolation and document business need~~ such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration);~~.~~ that enforces electronic access control and logical isolation and documents the business need.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.2	SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS ~~High Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~ Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	~~An e~~Examples of evidence may include, but is not limited to, ~~network diagrams showing all external routable communication paths and the identified EAPs~~documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.3	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS connected to a network via routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: • confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other nonprogrammable communication components, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE). ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of e~~Evidence may include, but is not limited to, architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption)~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason~~.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and ~~1.~~3. EACMS hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated: • PCS; • PACS; or • EACMS	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS at Control Centers and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PCA; • PACS, or • EACMS ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for~~ D~~d~~etect~~ing~~ known or suspected malicious Internet Protocol (IP) communications ~~for both inbound and outbound communications~~entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~Each~~ Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-8~~7~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • PCA SCI with IRA hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Ensure that ~~authorized~~ IRA is through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access applicable systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA	An example of evidence may include, but is not limited to, architecture

CIP-005-8~~7~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
	~~High Impact BES Cyber Systems and their associated:~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	between the client and the Intermediate System. ~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	documents detailing where ~~encryption~~ confidentiality and integrity controls initiate~~s~~ and terminate~~s~~.
2.3	Intermediate Systems used to access applicable systems of Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~2. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~3. PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8~~7~~ Table R2 – Remote Access Management

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

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access~~External Routable Connectivity~~ and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access.~~),such as:Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~

CIP-005-8~~7~~ Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.6	Intermediate Systems used to access applicable systems of Part 2.1	Implement for applicable systems as follows: **2.6.1.** Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	Examples of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~ 8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~ 8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~8~~7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable~~	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include

CIP-005-~~8~~7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Connectivity~~ERC SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS		terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.~~for both inbound and outbound communications. (1.5)~~	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~ 8 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. ~~have all applicable Cyber Assetssystems connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). protected by logical isolation~~ (Requirement R1 Part 1.1) OR The Responsible Entity did not ~~protect~~implement, for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability ~~the Management Systems or Management Interfaces or applicable systems per Requirement R1, Part 1.2External Routable Connectivity through the ESP was not through an identified EAP.~~ (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				nonprogrammable communication components ~~protect confidentiality and integrity of the data traversing communications links per Requirement R1, Part 1.3.The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default.~~ (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing D~~d~~ial-up ~~c~~Connectivity with the applicable ~~Cyber Assets~~systems~~, where technically feasible~~. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.		OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.5).	OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS,~~ and~~ SCI, and -Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS,~~ and~~ SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS,~~ and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS,~~ and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and ~~and~~ EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03~~
- CIP-005-8~~7~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21, 2021–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-006-7

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:

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

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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 BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:** See “Project 2016-02 Virtualization Implementation Plan.”

A. 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 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 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 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated Electronic Access Control or Monitoring System (EACMS) or Protected Cyber Asset (PCA); or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter 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 hosting High Impact BCS or their associated: • EACMS; or • PCA	Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters 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 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 hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
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 hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is 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 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-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	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 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCAs; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is 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 and additional evidence that the alarm or alerts was issued and communicated as identified in the BES 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-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated • EACMS; or • PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

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 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 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 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 hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with EERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter 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.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 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 hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety 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 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 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 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 BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter 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.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
	Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC		

B. 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 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-006-7)			
	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. (Requirement R1 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. (Requirement R1 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.

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 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 or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 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 visitor's name, and the point of contact. (Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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. (Requirement R3 Part 3.1)	and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	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. (Requirement R3 Part 3.1)	the Physical Security Perimeter. (Requirement R3 Part 3.1) OR 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 27 calendar months. (Requirement R3 Part 3.1)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

See "Project 2016-02 Virtualization Implementation Plan"

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

Version	Date	Action	Change Tracking
			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	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21, 2021–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. Number: CIP-006-7~~6~~

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-006-7~~6~~:

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~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2~~4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation 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~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates: See “Project 2016-02 Virtualization Implementation Plan.”

~~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:**~~

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

~~**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.~~

A. 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~~6~~ 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~~6~~ 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~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact ~~BES Cyber Systems~~BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS~~BES Cyber Systems, or~~ • Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated Electronic Access Control or Monitoring System (EACMS) or Protected Cyber Asset (PCA); or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter 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~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA	~~Where technically feasible, u~~Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters 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~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is 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 and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident ~~R~~response ~~P~~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-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	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~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCAs; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is 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 and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident ~~R~~response ~~P~~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-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated • EACMS; or • PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

~~CIP-006-6 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-006-7~~6~~ 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~~6~~ Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	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~~.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with E~~xternal Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter 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.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety 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~~6~~ 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~~6~~ Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ 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~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter 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.

CIP-006-7~~6~~ Table R3 – Physical Access Control System Maintenance and Testing Program

Part	Applicable Systems	Requirement	Measures
	associated EACMS or PCA; or - SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC		

B. 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 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-006-7~~6~~)			
	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. (Requirement R1 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. (Requirement R1 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.

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 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 or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6)

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption,~~

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~monitoring or equally effective logical 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. (Requirement R2 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 visitor's name, and the point of contact.

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 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. (Requirement R3 Part	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 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 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, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR 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 27 calendar months. (Requirement R3 Part

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	3.1)			3.1)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan"

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

Version	Date	Action	Change Tracking
			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	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-007-7

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:

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

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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 BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates:

See "Project 2016-02 Virtualization 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 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 Table R1* – System Hardening and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Enable only network accessible services that have been determined to be needed by the Responsible Entity (or logical network accessible ports if unable to determine service, including port ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files, command output (such as netstat), or network scans of open ports; or • Configuration of host-based firewalls, policy, or other mechanisms that only allow needed ports and deny all others.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated PCA. Medium Impact BCS at Control Centers and their associated PCASCI at Control Centers hosting High or Medium Impact BCS or their associated PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is 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.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Enable only services that have been determined to be needed by the Responsible Entity, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of implemented hardening guidelines • Configuration management reporting that demonstrates the need for all enabled services.

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 Table R2 – 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 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – 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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 systems that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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; • 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 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 patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System 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 security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BCS 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 SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • 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 of evidence may include, but is not limited to, records of implementation of mitigations.

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 Table R3 – Malicious Code Protection [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 Table R3 – Malicious Code Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection			
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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 of evidence may include, but is 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 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 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, 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; 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 BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated: • PACS • EACMS; or • PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, at 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 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 at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 days or greater.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA Management Modules of SCI hosting High BCS or their associated: • EACMS; or • PCA	Review a summarization or sampling of logged 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-007-7 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 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
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 External Routable Connectivity (ERC) and their associated:	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 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA		
5.2	High Impact BCS and their associated:	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).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use.

CIP-007-7 Table R5 – System Access Controls			
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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated • PACS; • EACMS; or • PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	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 SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 system; 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 system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots 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 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 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 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-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for System Hardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2)	The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for	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-007-7

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 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 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	tracking or evaluating cyber security patches for applicable systems. (Requirement R2 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 security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 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 patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65	installing cyber security patches for applicable systems. (Requirement R2 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 security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 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	Table R2. (Requirement R2) 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 systems. (Requirement R2 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

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	completion. (Requirement R2 Part 2.3)	calendar days of the evaluation completion. (Requirement R2 Part 2.3)	applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	delegate. (Requirement R2 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. (Requirement R2 Part 2.4)
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. (Requirement R3 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. (Requirement R3 Part 3.2)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R3. (Requirement R3).

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (Requirement R3 Part 3.3).	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. (Requirement R3 Part 3.1)
R4	The Responsible Entity has documented and implemented 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 interval and completed the review within 22	The Responsible Entity has documented and implemented 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 interval and completed the review within 30 calendar days of the prior review. (Requirement R4 Part 4.4)	The Responsible Entity has documented and 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 events described in 4.2.1	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4) OR The Responsible Entity has documented and implemented one or more process(es) to log

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of the prior review. (Requirement R4 Part 4.4)		through 4.2.2. (Requirement R4 Part 4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented 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	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. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			missed two or more intervals. (Requirement R4 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. (Requirement R5 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. (Requirement R5 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). (Requirement R5 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. (Requirement R5 Part 5.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 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. (Requirement R5 Part 5.1) OR

R #	Violation Severity Levels (CIP-007-7)			
	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. (Requirement R5 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. (Requirement R5 Part 5.5)	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. (Requirement R5 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. (Requirement R5 Part 5.4) OR

R #	Violation Severity Levels (CIP-007-7)			
	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 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. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR 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

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

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.	

Version	Date	Action	Change Tracking
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 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	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-007-7~~6~~

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~~4.1.4 ~~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:

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~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). ~~Electronic Security Perimeters.~~

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.2~~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.

~~4.2.3.3~~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~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-007-76).~~

~~**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:~~

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

~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 Table R1 –* System Hardening*~~Ports and Services~~*. *[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 Table R1 –* System Hardening*~~Ports and Services~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, E~~Enable only ~~logical~~ network accessible ~~ports~~ services that have been determined to be needed by the Responsible Entity~~,~~ (or logical network accessible ports if unable to determine service, including port ranges ~~or services~~ where needed to handle dynamic ports), per system capability. ~~-~~If a ~~device~~ system has no provision for disabling or restricting network accessible services (or logical ports) ~~on the device~~ then those ~~ports~~ services (or logical ports), that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, ~~on all applicable Cyber Assets and Electronic Access Points,~~ individually or by group. • Listings of the listening ports, ~~on the Cyber Assets,~~ individually or by group, from either ~~the device~~ configuration files, command output (such as netstat), or network scans of open ports; or • Configuration ~~files~~ of host-based firewalls,~~-~~ policy, or other ~~device level~~ mechanisms that only allow needed ports and deny all others.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA.~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated ~~:~~PCA~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is 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.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	Enable only services that have been determined to be needed by the Responsible Entity, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of implemented hardening guidelines - Configuration management reporting that demonstrates the need for all enabled services.

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~~6~~ Table R2 – 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~~6~~ Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 systems ~~for applicable Cyber Assets~~ that are updateable and for which a patching source exists.	An example of evidence may include, but is 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.~~.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 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 patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System 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 security patch and a timeframe for the completion of these mitigations.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact ~~BES Cyber Systems~~BCS 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 SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • 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 of evidence may include, but is not limited to, records of implementation of mitigations.

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~~6~~ Table R3 – Malicious Code Protection~~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~~6~~ Table R3 – Malicious Code Protection~~Prevention~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	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 of evidence may include, but is 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~~6~~ 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~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber A~~a~~sset level (per Cyber A~~a~~sset capability)~~ for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, at~~s~~ 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; 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 System~~ BCS 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 ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS or Medium Impact BCS ~~with ERC~~ or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated: • PACS • EACMS; or • PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, a~~s~~t a minimum, each of the following types of events, ~~(~~per system ~~or Cyber Aasset or BES Cyber 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.

4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	~~Where technically feasible,r~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system ~~or asset~~ 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 days or greater.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA Management Modules of SCI hosting High BCS or their associated: • EACMS; or • PCA	Review a summarization or sampling of logged 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-007-7~~6~~ 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~~6~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated:	Have a method(s) to enforce authentication of interactive user access, per system capability~~where technically feasible~~.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7 Table R5 – System Access Controls			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated:	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).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use ~~for the BES Cyber System~~.

CIP-007-~~6~~7 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

CIP-007-7~~6~~ Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated • PACS; • EACMS; or • PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Change known default passwords, per system ~~or Cyber Aasset~~ 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~~.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	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 SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	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 system~~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 system.~~Cyber Asset.~~	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots 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~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	~~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 screen~~-~~shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	~~Where technically feasible, either:~~ 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 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 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.

~~1.3. Compliance Monitoring and Assessment Processes:~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for ~~Ports and Services~~ System Hardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2)	The Responsible Entity has implemented and documented processes for determining necessary System Hardening~~Ports and Services but~~, ~~where technically feasible,~~ but had one or more unneeded ~~logical~~ network accessible services ~~ports~~ enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R1. (Requirement R1)
R2	The Responsible Entity has documented and	The Responsible Entity has documented or implemented one or	The Responsible Entity has documented or	The Responsible Entity did not implement or

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 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 patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days	more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 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 security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 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	implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable ~~Cyber Assets~~ systems. (Requirement R2 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 security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented	document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R2. (Requirement R2) 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~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but less than 50 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	applicable security patches, did not apply the applicable 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. (Requirement R2 Part 2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (Requirement R2 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. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but,	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	but did not mitigate the threat of detected malicious code. (Requirement R3 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. (Requirement R3 Part 3.3).	process(es) that included the applicable items in CIP-007-7~~6~~ 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. (Requirement R3 Part 3.1)
R4	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	The Responsible Entity has documented and implemented 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 interval	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R4. (Requirement R4)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	and completed the review within 30 calendar days of the prior review. (Requirement R4 Part 4.4)	device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 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 event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	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. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 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. (Requirement R5 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. (Requirement R5 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). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ 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

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not include the identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) 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. (Requirement R5 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	interactive user access. (Requirement R5 Part 5.1) 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. (Requirement R5 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.

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR 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 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)	(Requirement R5 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 Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	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 18 calendar months of the last password change. (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 the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

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.	

Version	Date	Action	Change Tracking
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 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	Virtualization modifications	

~~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:~~

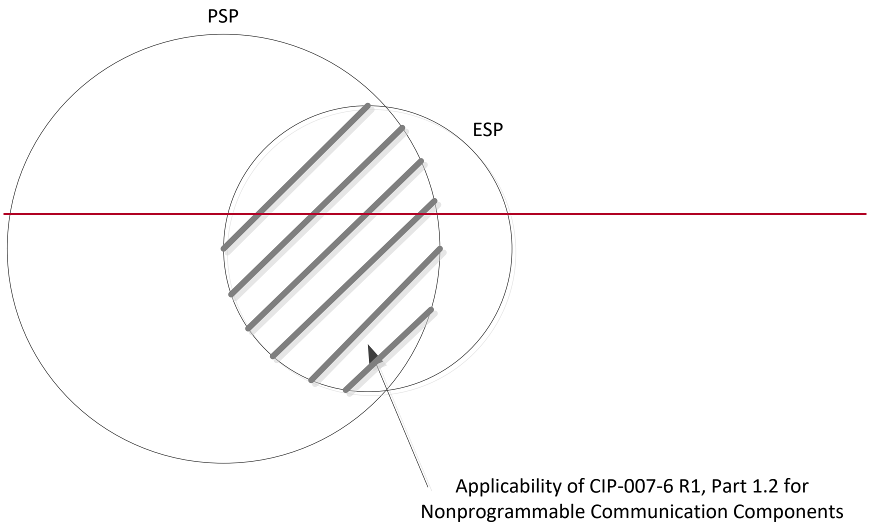
- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

~~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:~~

Location of Nonprogrammable Communication Components


PSP
ESP
Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

~~**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.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-008-7

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:

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 where the Remedial Action Scheme 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 where the Remedial Action Scheme 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:

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

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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 (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:**

See "Project 2016-02 Virtualization 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 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 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is 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.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS.	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 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 hosting High or Medium Impact BCS or their associated: - EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is 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 ImpactBCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is 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 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 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 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 hosting High or Medium Impact BCS or their associated: • EACMS	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.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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.
2.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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 of evidence may include, but is 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 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 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 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 hosting High or Medium Impact BCS or their associated: - EACMS	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 of evidence may include, but is not limited to, 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-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or 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 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.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes 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] 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 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 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 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 hosting High or Medium Impact BCS or their associated: • EACMS	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.

[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-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or 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: • 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 NCCIC.

CIP-008-7 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 hosting High or Medium Impact BCS or their associated: • EACMS	Provide updates, if any, within 7 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.

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 Enforcement 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 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. (Requirement R2 Part 2.2)	plan(s) within 18 calendar months between tests of the plan(s). (Requirement R2 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. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the	The Responsible Entity has not updated the Cyber Security	The Responsible Entity has neither documented lessons	The Responsible Entity has neither documented lessons

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (Requirement R3 Part 3.1.3)	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. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified 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. (Requirement R3 Part 3.1.3)	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. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated 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. (Requirement R3 Part 3.1.2) OR	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. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their 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 notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 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	The Responsible Entity failed to notify E-ISAC or NCCIC, 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 Part R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified in the “Applicable Systems” column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) 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 4.1 but failed to report on			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes after determination pursuant to Part 4.1. (Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”

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

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-008-7~~6~~

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:

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 where the Remedial Action Scheme 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 where the Remedial Action Scheme 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~~6~~:

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~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2~~4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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.

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

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-008-76.~~

~~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 row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "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.~~

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~~6~~ 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~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is 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.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS.	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~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is 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~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is 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~~6~~ 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~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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.
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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 of evidence may include, but is 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~~6~~ 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~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	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 of evidence may include, but is 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-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or 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 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.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes 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] 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~~6~~ 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~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	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.

[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-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or 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: • 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 NCCIC.

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Provide updates, if any, within 7 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.

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~~ Enforcement 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.

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

~~**1.4. Additional Compliance Information:**~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning	Lower	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the “Applicable Systems” column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response	The Responsible Entity has not tested the Cyber Security Incident response

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 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. (Requirement R2 Part 2.2)	plan(s) within 18 calendar months between tests of the plan(s). (Requirement R2 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. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the	The Responsible Entity has not updated the Cyber Security	The Responsible Entity has neither documented lessons	The Responsible Entity has neither documented lessons

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (Requirement R3 Part 3.1.3)	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. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified 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. (Requirement R3 Part 3.1.3)	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. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated 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. (Requirement R3 Part 3.1.2) OR	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. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) - Roles or responsibilities, or - Cyber Security Incident response groups or individuals, or - Technology changes.	The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) - Roles or responsibilities, or - Cyber Security Incident response groups or individuals, or - Technology changes.	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their 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 notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 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	The Responsible Entity failed to notify E-ISAC or NCCIC, 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 Part R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified in the “Applicable Systems” column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) 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 4.1 but failed to report on			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes after determination pursuant to Part 4.1. (Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan."

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

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of 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-009-7:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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-002-7 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:** See "Project 2016-02 Virtualization 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 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 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	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).

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	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.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	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.	An example of evidence may include, but is 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 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 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BBCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 of evidence may include, but is 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.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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.	An example of evidence may include, but is 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-009-7 Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.3	High Impact BCS SCI hosting 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. 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 in *CIP-009-7 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 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS: and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 of evidence may include, but is 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.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BSC at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 defined role in the recovery plan of the updates.	An example of evidence may include, but is 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: • 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 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-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for applicable systems. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.
R2.	The Responsible Entity has not tested the recovery plan(s)	The Responsible Entity has not tested the recovery plan(s) within 16 calendar	The Responsible Entity has not tested the recovery plan(s)	The Responsible Entity has not tested the recovery plan(s) according to R2 Part

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested	months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Requirement R2 Part 2.3)	according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar	2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)		months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified 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. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated 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. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	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 recovery plan test or actual recovery. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 Virtualization Implementation Plan."

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.	

Version	Date	Action	Change Tracking
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	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-009-7~~6~~

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of 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 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~~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.

4.2.1.3. 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~~6~~:

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~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-7~~5.1~~ identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan" ~~for CIP-009-~~7~~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:~~

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

~~**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 in *CIP-009-7~~6~~ 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~~6~~ Table R1 – Recovery Plan Specifications*.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	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).

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: ● PACS; or ● EACMS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes for the backup and storage of information required to recover ~~BES Cyber System~~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 System~~ applicable system functionality.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: ● PACS; or ● EACMS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes to preserve data, per ~~Cyber Asset~~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.	An example of evidence may include, but is 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~~6~~ 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~~6~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact B~~ES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 of evidence may include, but is 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.

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: ● PACS; or ● EACMS	Test a representative sample of information used to recover ~~BES Cyber System~~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 System~~applicable system functionality substitutes for this test.	An example of evidence may include, but is 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-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS SCI hosting High Impact ~~BES Cyber Systems~~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 in *CIP-009-7~~6~~ 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~~6~~ Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS: and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 of evidence may include, but is 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.

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BSC at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	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 defined role in the recovery plan of the updates.	An example of evidence may include, but is 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: • 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 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.

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

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

~~**1.5. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~BES Cyber Systems~~applicable systems. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)	months between tests. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified 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. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated 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. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in	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 recovery plan test or actual recovery. (Requirement R3 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 each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated 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: (Requirement R3 Part 3.2)	

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			• Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan."

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.	

Version	Date	Action	Change Tracking
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	Virtualization conforming changes	

~~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~~

~~Installation files and media;~~

~~Current backup tapes and any additional documented configuration settings;~~

~~Documented build or restoration procedures; and~~

~~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.~~

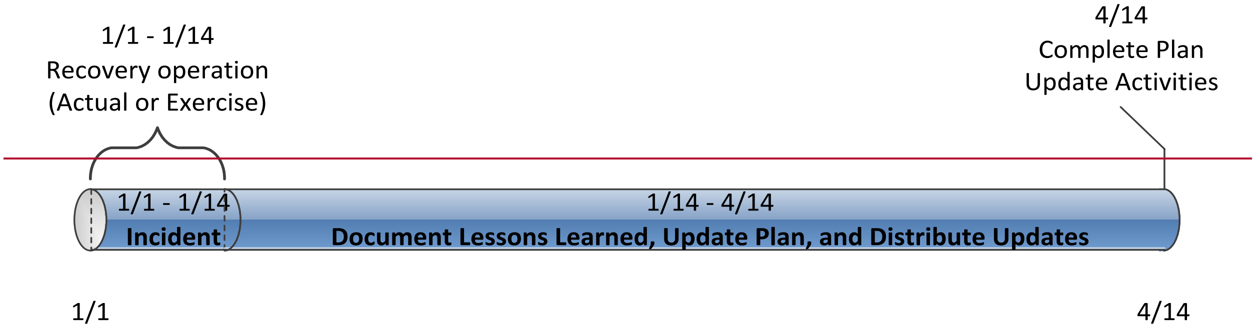
~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (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.~~

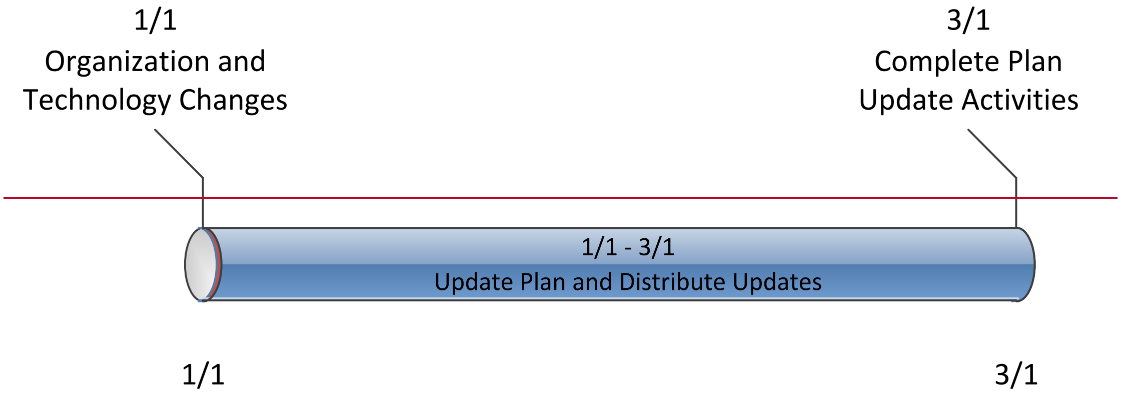
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take 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.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-010-5

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

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

Effective Date: See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Authorize changes to: 1.1.1. Operating system(s) or firmware or images used to derive operating systems or firmware; 1.1.2. Commercially available or open-source application software including Self-Contained Applications; 1.1.3. Custom software installed including Self-Contained Applications; 1.1.4. Any logical network accessible services, (or logical ports if unable to determine service); 1.1.5. Security patches applied; 1.1.6. SCI configuration that:	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change.

CIP-010-5 Table R1 – Change Management

Part	Applicable Systems	Requirements	Measures
	Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	- Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; - Enforces logical isolation between systems with different impact ratings hosted on SCI; - Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or - Enables or disables SCI services.	
1.2	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	For each change to the items listed in Part 1.1: 1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.2.2. Following the change, verify that required cyber security controls determined in 1.2.1 are not	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	adversely affected; and 1.2.3. Document the results of the verification.	
1.3	High Impact BCS SCI hosting High Impact BCS	For each change to the items listed in Part 1.1, per system capability: 1.3.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.3.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS	Prior to a change associated with Requirement Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.4.1. Verify the identity of the software source; and 1.4.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.4: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.		

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Change Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for unauthorized changes to the items described in Requirement R1, Part 1.1. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table*.*

CIP-010-5 Table R3 – Vulnerability Assessments			
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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BES Cyber Systems or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High Impact BCS or their associated: • EACMS; or • PCA	Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability, except for CIP Exceptional Circumstances, or deployments using a previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

3.4	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 hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a report of Management System actions, or a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

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

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

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a change management process(es) that includes only four or more of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change management process(es) that includes only three of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change management process(es) that includes only two of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity has a process as specified in Part 1.4 to verify the identity of the software source (1.4.1) but does not have a process as specified in Part 1.4 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.4.2)	The Responsible Entity has not documented or implemented any change management process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a change management process(es) that includes only one of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change management process(es) that requires authorization of changes to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a process(es) to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration. (Requirement R1 Part 1.2.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration but did not verify and document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.2.2 & Part 1.2.3) OR The Responsible Entity does not have a process for testing changes prior to implementing a change

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				tothe configuration. (Requirement R1 Part 1.3.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (Requirement R1 Part 1.3.2) OR The Responsible Entity does not have a process as specified in Part 1.4 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable systems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	vulnerability assessment processes for applicable systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	vulnerability assessment processes for applicable systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	vulnerability assessment processes for applicable systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for applicable systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable systems, but did not perform the active vulnerability assessment of its applicable systems. (Requirement R3 Part 3.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-5, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-5, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-5, Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-5, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”.
- CIP-010-5 Technical Rationale

Version History

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

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

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

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 3. Removable Media

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

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

3.1.2. Locations, either individually or by group.

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

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

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting to a BES Cyber System or Protected Cyber Assets; and

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

CIP-010-5 - Attachment 2

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

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

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

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

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

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

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

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

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

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

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-010-5~~4~~

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

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5~~4~~:

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~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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.

4.2.3.6. 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" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

~~5.~~ **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan." ~~for Project 2019-03.~~

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

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

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

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident~~

~~response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

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

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

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

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

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

~~**"Applicable Systems" Columns in Tables:**~~

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

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

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

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

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

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 –~~ Configuration~~ Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 –~~ Configuration~~ Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Authorize changes to~~Develop a baseline configuration, individually or by group, which shall include the following items~~: 1.1.1. Operating system(s)~~ (including version)~~ or firmware ~~where no independent operating system exists~~or images used to derive operating systems or firmware; 1.1.2. ~~Any c~~Commercially available or open-source application software ~~(including version) intentionally installed~~including Self-Contained Applications; 1.1.3. ~~Any c~~Custom software installed including Self-Contained Applications; 1.1.4. Any logical network accessible ~~ports~~services, (or logical ports if unable to determine service);	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change. ~~A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~

CIP-010-54 Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	~~and~~ 1.1.5. ~~Any s~~Security patches applied;~~.~~ 1.1.6. SCI configuration that: - Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; - -Enforces logical isolation between systems with different impact ratings hosted on SCI; - Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or - Enables or disables SCI services.	
~~1.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~1. PACS; and~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ - ~~A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each~~

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~0. PACS; and~~ ~~0. PCA~~		~~change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~**1.3**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
1.2~~4~~	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For ~~a~~ each change ~~that deviates from the existing baseline configuration~~to the items listed in Part 1.1: 1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.2.2. Following the change, verify that required cyber security controls determined in 1.2~~4~~.1 are not	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	adversely affected; and 1.2.3. Document the results of the verification.	
1.3~~5~~	High Impact BCS SCI hosting High Impact BCS	~~Where technically feasible, f~~For each change ~~that deviates from the existing baseline configuration~~to the items listed in Part 1.1, per system capability: 1.3.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment -or test the	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.3.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.~~6~~4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS	Prior to a change ~~that deviates from the existing baseline configuration~~ associated with ~~baseline items in~~Requirement Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.4~~6~~.1. Verify the identity of the software source; and 1.4~~6~~.2. Verify the integrity of the software obtained from the	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-54 Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.4~~6~~: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	software source.	

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~4~~ 5 Table R2 – ~~Configuration~~ Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~ 5 Table R2 – ~~Configuration~~ Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R2 – ~~Configuration~~ Change Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for unauthorized changes to the ~~baseline configuration (as~~items described in Requirement R1, Part 1.1~~)~~. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~4~~ 5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BES Cyber Systems or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High Impact BCS or their associated: • EACMS; or • PCA	Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability~~Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset~~, except for CIP Exceptional Circumstances, or ~~and like replacements~~deployments ~~of the same type of Cyber Asset with~~using a ~~baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset~~previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

3.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a report of Management System actions, or a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

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

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

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only four or more of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only three of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only two of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1) OR The Responsible Entity has a process as specified in Part 1.~~6~~4 to verify the identity of the software source (1.~~6~~4.1) but does not have a process as specified in Part 1.~~6~~ 4 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.~~6~~4.2)	The Responsible Entity has not documented or implemented any ~~configuration~~ change management process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only one of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change management process(es) that requires authorization ~~and documentation~~ of changes ~~that deviate from the existing baseline~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~configuration~~to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.1~~2~~) ~~OR~~ ~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration. (Requirement R1 Part 1.~~4~~2.1) OR The Responsible Entity has a process(es) to determine required security controls in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration but did not verify and document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.~~4~~2.2 & Part 1.~~4~~2.3) OR The Responsible Entity does not have a process for testing changes ~~in an environment that models the baseline configuration~~ prior to implementing a change ~~that deviates from baseline~~to the configuration. (Requirement R1 Part 1.~~5~~3.1) OR The Responsible Entity does not have a process to document the test results and, if using a test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				environment, document the differences between the test and production environments. (Requirement R1 Part 1.~~5~~3.2) OR The Responsible Entity does not have a process as specified in Part 1.~~6~~4 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.~~6~~4)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the baseline~~ at least once every 35 calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~A~~applicable s~~S~~ystems, but has performed an active vulnerability assessment more than 36 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 39 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 42 months, but	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable ~~BES Cyber S~~systems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	less than 39 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	less than 42 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	less than 45 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable ~~BES Cyber S~~systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration~~ of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-~~4~~5, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-~~4~~5, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-~~4~~5, Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-~~4~~5, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-45, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03~~.
- CIP-010-~~4~~ 5 Technical Rationale

Version History

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

CIP-010-5~~4~~ - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

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

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 3. Removable Media

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

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

3.1.2. Locations, either individually or by group.

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

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

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

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

CIP-010-~~4~~5 - Attachment 2

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

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

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

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

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

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

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

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

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

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

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

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

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

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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.

5. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

6. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection*. *[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 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS.	Method(s) to identify information that meets the definition of BCSI.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BCSI from 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 recognize BCSI; or • Repository or electronic and physical location designated for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS	Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include 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).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 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-011-3 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • EACMS; • PACS; or • PCA	Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).	Examples of acceptable evidence include, but are not limited to: • 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 or other methods used to prevent unauthorized retrieval of BCSI.

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 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)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BCSI protection program (Requirement R1).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. (Requirement R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.

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	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

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

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems 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-011-3~~2~~:

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~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation 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.

4.2.3.6. 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. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Dates: See "Project 2016-02 Virtualization Implementation Plan." ~~for CIP-011-3~~2~~.~~

~~**6. 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:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and~~

~~Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “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.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

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

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection*. *[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~~2~~ Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3~~2~~ Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS.	Method(s) to identify information that meets the definition of ~~BES Cyber System Information~~BCSI.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify ~~BES Cyber System Information~~BCSI from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize ~~BES Cyber System Information~~BCSI; or • Repository or electronic and physical location designated for housing ~~BES Cyber System Information~~BCSI in the entity's information protection program.

CIP-011-3~~2~~ Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS	Procedure(s) for protecting and securely handling ~~BES Cyber System Information~~BCSI, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of ~~BES Cyber System Information~~BCSI; or • Records indicating that ~~BES Cyber System Information~~BCSI is handled in a manner consistent with the entity's documented procedure(s).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3~~2~~ 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-011-3~~2~~ Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

CIP-011-3~~2~~ 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. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence include, but are not limited to:~~ ~~• 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 BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

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 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.

~~**1.1. Compliance Monitoring and Assessment Processes:**~~

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

~~**6.1. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-011~~0~~-3~~2~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a ~~BES Cyber System Information~~BCSI protection program (Requirement R1).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the BES Cyber Asset. (Requirement R2 Part 2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the BES Cyber Asset. (Requirement R2 Part 2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal. (Requirement R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan. ~~Guideline and Technical Basis (attached).~~

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	TBD	Virtualization conforming changes	

~~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:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~**Requirement R2:**~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

~~quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization~~ processes.

~~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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Rationale for Requirement R2:~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** **CIP-013-3~~2~~**

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

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3~~2~~:

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)~~logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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 identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan." ~~for Project 2019-03.~~

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan” f~~or Projec~~t ~~2019-03~~
- ~~CIP-013-2 Technical Rationale~~

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** **CIP-013-3**

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

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation 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 identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	R1 Part 1.2.1 through Part 1.2.6.	Requirement R1 Part 1.2.1 through Part 1.2.6.		The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan” ft

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Agenda Item 7
Standards Committee
January 20, 2021

Standard Authorization Request
Operational Data Exchange Simplification

Action

- Accept the Standard Authorization Request (SAR) that was submitted by the Standards Efficiency Review team proposing to enhance the effective and efficient administration of operational data exchange required by NERC Reliability Standards IRO-010-2[1] and TOP-003-3;[2]
- Authorize posting of the SAR for a 30-day formal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members.

Background

As stated in the SAR, the primary purpose of this project is to simplify administrative burdens and limit unnecessary data requirements that do not contribute to BES reliability and resiliency. As written the standards create a zero-defect expectation for each Registered Entity receiving a data specification to demonstrate perfect performance on every item in the data specification for an entire audit period. This can result in unnecessary administrative burdens for the Registered Entity to demonstrate compliance, including excessive data retention. A secondary purpose of this project is to evaluate and, if necessary, remove potentially redundant data exchange requirements dispersed in other standards.

Summary

The scope of the proposed project is to simplify the administrative burden with IRO-010-2 and TOP-003-3 by developing risk-based compliance expectations and clarifying the four tasks identified in IRO-010-2 and TOP-003-3 (i.e., Operational Planning Analysis, Real-time Assessment, Real-time monitoring, Balancing Authority analysis functions). The project may require revisions to associated definitions and other standards as necessary to clarify expectations and remove redundant obligations. The project may also require development of Implementation Guidance or other ERO guidance to simplify the administrative burden. The project should include coordination with existing projects that have operational data exchange within their scope (including Projects 2015-09 and 2019-06).

[1] IRO-010-2, Reliability Coordinator Data Specification and Collection, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=IRO-010-2&title=Reliability%20Coordinator%20Data%20Specification%20and%20Collection&jurisdiction=United%20States

[2] TOP-003-3, Operational Reliability Data, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=TOP-003-3&title=Operational%20Reliability%20Data&jurisdiction=United%20States

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda item 7a
Standards Committee
January 20, 2021

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Operational Data Exchange Simplification		
Date Submitted:	June 23, 2020		
SAR Requester			
Name:	Standards Efficiency Review Phase 2 Team (John Allen)		
Organization:	City Utilities of Springfield		
Telephone:	417-831-8972	Email:	John.Allen@cityutilities.net
SAR Type (Check as many as apply)			
□ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☒ Withdraw/retire an Existing Standard		□ Imminent Action/ Confidential Issue (SPM Section 10) □ Variance development or revision ☒ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
□ Regulatory Initiation □ Emerging Risk (Reliability Issues Steering Committee) Identified □ Reliability Standard Development Plan		□ NERC Standing Committee Identified □ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The proposed project will enhance the effective and efficient administration of operational data exchange for the purpose of focusing operating personnel on safe, secure and reliable operations.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
The primary purpose of this project is to simplify administrative burdens identified by the SER Phase 2 Team associated with the current IR0-010-2 and TOP-003-3 standards and limit unnecessary data requirements that do not contribute to BES reliability and resiliency. As written the standards create a zero-defect expectation for each Registered Entity receiving a data specification to demonstrate perfect performance on every item in the data specification for an entire audit period. This can result in unnecessary administrative burdens for the Registered Entity to demonstrate compliance, including excessive data retention. If instead a risk-based approach was developed and performance was			

Requested information

triggered upon an event or unresolved data conflicts between entities, then the purpose of the standards would be achieved in an effective and efficient manner.

Therefore, the industry would benefit from continuing the efforts of Project 2014-03 and further revising IR0-010-2 and TOP-003-3 to enhance the “data specification” approach to ensuring Registered Entities with operational responsibilities request and receive any data necessary to support the four tasks identified in IRO-010-2 and TOP-003-3 and described in the Detailed Description section below, while protecting public disclosure of commercially sensitive information. To preserve the “data specification” concept, flexibility for differences in operational environments and emerging technology must be maintained. Therefore, creating a minimum list of items to include in a data specification is not desired. However, more clarity regarding the scope of the four tasks identified in IRO-010-2 and TOP-003-3 would be beneficial and is desired. The scope of the data specification would then just reflect the information necessary to cover the scope of the applicable tasks identified in IRO-010-2 or TOP-003-3 for the individual Registered Entity. The SER Phase 2 team received some feedback from industry participants who believe the scope of a data specification would only contain routine real time operating data typically provided systematically from field devices via SCADA/ICCP. Therefore, it is also necessary to clarify for industry if it should contain other data/information and methods of transfer such as phone, instant messaging, internet-based systems, etc.

A secondary purpose of this project is to evaluate removing other data exchange requirements dispersed in other standards. The drafting team would need to evaluate those requirements after proposed changes to the IR0-010 and TOP-003 are developed to determine if they are within the scope of the four tasks and consequently within the scope of IRO-010 and TOP-003. This may require enhancing the standards to allow each Registered Entity with responsibilities to perform the tasks identified in IRO-010-2 and TOP-003-3 the ability to request and receive any information it needs from other Registered Entities to perform those tasks.

Project Scope (Define the parameters of the proposed project):

The scope of the proposed project is to simplify the administrative burden with IRO-010-2, TOP-003-3 by developing risk-based compliance expectations and clarifying the four tasks identified in IRO-010-2 and TOP-003-3. The proposed project will need to utilize any available industry resource necessary to maintain flexibility for various operational environments and technology. The project will require revisions to IRO-010-2, TOP-003-3 and associated definitions (especially Real-time monitoring and Balancing Authority analysis functions) and may also require development of Implementation Guidance or other ERO guidance to simplify the administrative burden. The proposed project may also require revisions to other standards as necessary to clarify expectations and remove redundant obligations. The scope of the project should also include coordination with existing projects that have operational data exchange within their scope including projects 2015-09 and 2019-06.

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition).
The project will, at a minimum, require revisions to IRO-010-2, TOP-003-3 and associated definitions in the NERC Glossary (especially Real-time monitoring and Balancing Authority analysis functions) to clarify expectations for the “data specification” and associated tasks identified in IRO-010-2 and TOP-003-3. The revisions should allow each Registered Entity with operational responsibilities to perform the tasks identified in IRO-010-2 and TOP-003-3 the ability to request and receive any information it needs to perform those tasks, while protecting public disclosure of commercially sensitive information. The four tasks identified in IRO-010-2 and TOP-003-3 and associated standards are listed below. • Operational Planning Analysis (IRO-008-2 and TOP-002-4) • Real-time Assessments (IRO-008-2 and TOP-001-4) • Real-time monitoring (IRO-002-5 and TOP-001-4) • Balancing Authority analysis functions (BAL-001-2, BAL-002-3, BAL-003-1.1 and BAL-005-1) This may necessitate revisions to the standards included above and any other standard or definition identified by the drafting team during the project as necessary to achieve the purpose of this project. The drafting team should also coordinate with pre-qualified organizations to develop Implementation Guidance and/or NERC staff to develop other ERO guidance to simplify the administrative burden. Once those activities are clarified, the drafting team should also evaluate and, if necessary, remove potentially redundant operational data exchange requirements dispersed in other standards including the following: • BAL-005-1 R2 • EOP-005-3 R13 • EOP-005-3 R14.2 • FAC-014-2 R5 • FAC-014-2 R6.1. • IRO-008-2 R5 • IRO-008-2 R6 • IRO-017-1 R3

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information

- TOP-001-4 R9
- TOP-001-4 R15
- VAR-002-4.1 R3
- VAR-002-4.1 R4

The project should also evaluate any other standard identified by the drafting team during the project as necessary to achieve the purpose of this project. The drafting team should seek to identify opportunities to remove redundant requirements and if necessary, retire requirements that are not needed for reliability. The evaluation at a minimum should consider the following questions:

- Is the purpose of the activity currently within the scope of one or more of the tasks and consequently IRO-010-2 and TOP-003-3? If so, then remove as redundant.
- If minor modifications were made to IRO-010-2, TOP-003-3 and/or associated definitions (especially Real-time monitoring and Balancing Authority analysis functions), then would the activity be within the scope of those standards? If so, then revise and remove as redundant.
- Does the receiving Registered Entity have an obligation to use the information? If so, then identify the existing requirement or create a new requirement for them to use it. If not, then retire outright as unnecessary for reliability of the BES.

The drafting team should reference precedence from past projects to support this effort, including background materials developed during Project 2014-03 that describe the “data specification” concept including the petition to the FERC and the Project 2014-03 Mapping Document.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

unknown

Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):

N/A

To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):

All NERC Functional Entities are potentially impacted by the scope of this SAR. The recommendations are both technical and administrative in nature but meant to address inefficiencies within requirements for data collection. Therefore, the drafting team should consist of members who are familiar with both aspects.

Requested information
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The SER Phase 2 team hosted an industry webinar on February 22, 2019 presenting six efficiency concepts, including consolidating and simplifying information and data requirements. The presentation was followed up by an industry survey to assess support for the concepts. This concept received the second highest support from industry. In addition, an informal survey was conducted on the content of this SAR to assess industry support. The feedback from industry and SER Phase 2 team responses are located on the Standards Efficiency Review page.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Yes, Projects 2015-09 and 2019-06.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
Yes, Implementation Guidance and/or other ERO guidance could assist with simplifying the administrative burden for the interim period while this project is being administered.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
□	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
□	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
□	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
□	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
□	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
□	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
□	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk

Agenda Item 8
Standards Committee
January 20, 2021

Standard Authorization Request
Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability

Action

- Accept the Standard Authorization Request (SAR) from the NERC Power Plant Modeling Verification Task Force (PPMVTF) to address the issues that exist with MOD-025-2[1] regarding verification and data reporting of generator active and reactive power capability;
- Authorize posting of the SAR for a 30-day informal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members.

Background

The PPMVTF developed this SAR to revise MOD-025-2 to address issues regarding verification and data reporting of generator active and reactive power capability. As stated in the SAR, implementation of the standard has rarely produced data that is suitable for planning models (i.e., the stated purpose of the standard). The current MOD-025-2 verification testing activities require significant time, expertise, and coordination; however, they do not result in data that should be used by planners for modeling purposes. The SAR aims to retain testing activities are useful and focus on more effective means of collecting useful data for planning models.

The Reliability, Security, and Technology Committee (RSTC) endorsed the SAR on October 19, 2020.

Summary

The intent of this standard revision project is to address the issues that exist with MOD-025-2 regarding verification and data reporting of generator active and reactive power capability (and any other relevant equipment capability). The vast majority of testing cases are limited by limits within the plant or system operating conditions that prohibit the generating resource from reaching its “composite capability curve” – the equipment capability or associated limiters.

The primary reliability benefit of this project will be to correct these issues such that suitable and accurate data can be established through the verification activities performed by respective equipment owners. Bulk Power System planning assessments rely on accurate data, including machine active and reactive power capability, to identify potential reliability risks and develop mitigating actions for those risks.

[1] MOD-025-2, Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=MOD-025-2&title=Verification%20and%20Data%20Reporting%20of%20Generator%20Real%20and%20Reactive%20Power%20Capability%20and%20Synchronous%20Condenser%20Reactive%20Power%20Capability&jurisdiction=United%20States

Agenda Item 8a
Standards Committee
January 20, 2021

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	MOD-025-2 Verification and Data Reporting of Generator Capability		
Date Submitted:	10/19/2020		
SAR Requester			
Name:	Shawn Patterson, Chair		
Organization:	NERC Power Plant Modeling Verification Task Force (PPMVTF)		
Telephone:	303-445-2311	Email:	spatterson@usbr.gov

SAR Type (Check as many as apply)

☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan	☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The current industry need for this standards project is that industry implementation of MOD-025-2 has not resulted in useful unit capability data being provided for planning models of generating resources and synchronous condensers (i.e., the purpose statement of the standard). The primary reliability benefit of this project will be to correct these issues such that suitable and accurate data can be established through the verification activities performed by respective equipment owners. BPS planning assessments rely on accurate data, including machine active and reactive power capability, to identify potential reliability risks and develop mitigating actions for those risks.

The current MOD-025-2 verification testing activities require significant time, expertise, and coordination; however, they do not result in data that should be used by planners for modeling purposes. The current standard does allow for optional calculations to be performed to help facilitate better information sharing; however, calculations are not required nor can be used in many cases when auxiliary equipment limits or system operating conditions prohibit reaching the actual machine capability or limiters. This standards project will address these issues.

Requested information

Other benefits of this standards project to address issues with MOD-025-2 include, but are not limited to, the following:

- Preventing over- or under-estimation of generating facility active and reactive power, which could lead to potential reliability risks or unnecessary and expensive solutions to mitigate
- Identifying limitations within a generating facility that could constrain the resource from reaching the expected active/reactive capability at any given time
- More clearly communicating the necessary data to be used for modeling the respective resources in steady-state power flow models
- Ensure that the data users are part of the verification process to ensure that the necessary and usable data is provided and utilized appropriately
- Ensure that raw test data alone is not used for resource modeling, but is analyzed, adjusted, and contextualized to account for measured system conditions
- Coordinating with PRC-019 activities to develop a composite capability curve, inclusive of equipment capabilities, limiters, and other plant limitations to develop an appropriate capability curve
- Ensuring that other means of verification (other than testing) can be more effectively leveraged to gather necessary and suitable data for verifying plant/machine capability

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

The intent of this standard revision project is to address the issues that exist with MOD-025-2 regarding verification and data reporting of generator active and reactive power capability (and any other relevant equipment capability). Currently, implementation of the standard rarely produces data that is suitable for planning models (i.e., the stated purpose of the standard). The vast majority of testing cases are limited by limits within the plant or system operating conditions that prohibit the generating resource from reaching its “composite capability curve” – the equipment capability or associated limiters. The goal of the proposed project is to:

- Ensure that testing and other verification activities produce useful data for verification of plant active and reactive power capability
- Ensure that the data is used by Transmission Planners and Planning Coordinators in an appropriate manner, with a sufficient degree of analysis prior to use
- Ensure that the data is applicable and usable by the Transmission Planner and Planning Coordinator for reliability studies
- Ensure Generator Owners appropriately identify limits within their generating resources (and synchronous condensers), and effectively communicate those limits to Transmission Planners and Planning Coordinators for the purposes of modeling these resources in reliability studies

Requested information

Project Scope (Define the parameters of the proposed project):

The scope of this project is to modify MOD-025-2 to ensure that data provided through verification activities performed by applicable Generator Owner or Transmission Owners produce suitable data for the purposes of developing accurate planning models in Transmission Planner and Planning Coordinator reliability studies. The project should consider, at a minimum, the following:

1. Revisions to MOD-025-2 to ensure that verification activities produce data and information that can be used by Transmission Planners and Planning Coordinators for the purposes of developing accurate and reasonable plant active and reactive capability data (including possibly representation of the “composite capability curve” inclusive of capability and limiters, where applicable).
2. Ensure that each Planning Coordinator and the area Transmission Planners develop requirements for the Planning Coordinator area real and reactive capability data verification
3. Ensure that Generator Owners provide the data specified by the Planning Coordinator and Transmission Planners for the Planning Coordinator area
4. Ensure that verification activities can apply other methods beyond only testing (or real-time data) that allow plant capability information, protection settings, PRC-019 reports, and other documentation to also complement the verification activities
5. Ensure that data provided by the applicable Generator Owners and Transmission Owners is analyzed and used appropriately by Transmission Planners and Planning Coordinators
6. Ensure that the data provided by Generator Owners, if different from tested values, is acceptable to the Planning Coordinator and Transmission Planners with the standard providing guidance on acceptable reactive capability reporting if system conditions prevent reaching actual capability.
7. Ensure alignment of the MOD-025 standard with MOD-032-1 regarding data submittals for annual case creation and PRC-019-2 regarding collection of information that can be effectively used for verification purposes. Ensure activities across standards can be applied to effectively meet the purpose of these standards, and avoid any potential overlap or duplication of activities. This is dependent on the success of bullet number 1.
8. Ensure that equipment limitations are documented and classified as expected (e.g., system voltage limit reached) or unexpected (e.g., plant tripped or excitation limiter reached unexpectedly). In cases of unexpected limitations reached, ensure that the equipment owner develops and implements a corrective action plan to address this unexpected limitation.

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
The NERC PPMVTF developed *White Paper: Implementation of NERC Standard MOD-025-2*[2] that recommends NERC initiate a standards project to address these issues with MOD-025-2. The white paper provides a detailed description and technical justification of the gaps that exist in MOD-025-2 and how the current standard may be leading to inaccurate data being used in BPS reliability studies. Further, the NERC PPMVTF *Reliability Guideline: Power Plant Model Verification and Testing for Synchronous Machines*[3] also describes in detail how testing activities per MOD-025-2 can lead to unusable data, and provides further guidance that a SDT could use to develop solutions to these issues.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The aforementioned NERC PPMVTF *White Paper: Implementation of NERC Standard MOD-025-2* includes an example of one Registered Entity's MOD-025 implementation costs (excluding cost of shifting the optimization of generation fleet assets due to minimum load testing requirements). The entity's average test cost was $1,259 (897 tests) and $4,326 per generator (261 generators). The verification testing of units generally results in transferring energy to a higher cost resource during the test period. Further, the data produced is often NOT suitable for planning studies, which does not serve the intended purpose of the standard and makes the added cost unjustified.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
The current MOD-025-2 was written around synchronous generation, although it is not specifically applicable only to synchronous generators. Therefore, the project should ensure the language is clear and concise regarding how to handle BES dispersed generating resources (e.g., wind, solar photovoltaic, and battery energy storage systems).
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
• Generator Owner and Transmission Owner of synchronous condensers (asset owner that is in the best position to ascertain resource capability)

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] https://www.nerc.com/comm/PC/Power%20Plant%20Modeling%20and%20Verification%20Task%20Force/PPMVTF_White_Paper_MOD-025_Testing.pdf

[3] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_PPMV_for_Synchronous_Machines_-_2018-06-29.pdf

Requested information

- Transmission Planner and Planning Coordinator (user of the information provided by the Generator Owner; currently has no responsibility of ensuring accurate data per current MOD-025-2 standard)

Do you know of any consensus building activities[4] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.

The NERC PPMVTF White Paper, approved by NERC RSTC, details the challenges with MOD-025-2. The team deliberated this subject for a significant amount of time, and have identified major issues with the standard that need to be addressed by an SDT. The PPMVTF believes that a significant revision to MOD-025-2 is needed, that testing activities are useful and should be retained, but that the activities can focus on more effective means of collecting useful data for planning models. One dissenting opinion of PPMVTF membership believed the standard should be retired completely and not replaced with an alternative.

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

The NERC standards development Project 2020-02 (Transmission-connected Dynamic Reactive Resources) SAR includes MOD-025-2, specifically addressing the applicability of transmission connected reactive devices in addition to generators and synchronous condensers.

The SAR on PRC-019-2 submitted to NERC by the System Protection and Control Subcommittee is also related in that there is significant overlap of activities in PRC-019-2 and the development of planning models of machine capability.

This SAR could be combined with those portions of those SARs to address this problem effectively.

Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

There are two key industry reference documents on this subject:

1. NERC *Reliability Guideline: Power Plant Model Verification and Testing for Synchronous Machines*[5] (July 2018) that provides recommended practices for synchronous machine capability testing. An appendix is devoted to MOD-025-2 testing, and highlights the challenges and inherent errors in MOD-025-2 to obtain useful data that can be applied for planning models.
2. NATF *Modeling Reference Document Reporting and Verification of Generating Unit Reactive Power Capability for Synchronous Machines*[6] (April 2015) that describes testing activities per MOD-025-2 and means of ensuring data is sufficient for planning studies.

[4] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

[5] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_PPMV_for_Synchronous_Machines_-_2018-06-29.pdf

[6] https://www.natf.net/docs/natf/documents/resources/planning-and-modeling/natf-reference-document-reporting-and-verification-of-generating-unit-reactive-power-capability-for-synchronous-machines.pdf

Requested information
Neither industry reference document addresses the identified shortcomings of the standard described above and in NERC PPMVTF *White Paper: Implementation of NERC Standard MOD-025-2*.[7] These reference materials help industry understand how to implement the standards using best practices, but do not address the reliability gaps created by the standard requirements themselves which is leading to inaccurate data being used in planning assessments.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes

[7] https://www.nerc.com/comm/PC/Power%20Plant%20Modeling%20and%20Verification%20Task%20Force/PPMVTF_White_Paper_MOD-025_Testing.pdf

Market Interface Principles	
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
N/A	None identified.

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 9
Standards Committee
January 20, 2021

Standard Authorization Request
Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

Action

- Accept the Standard Authorization Request (SAR) submitted by NERC System Protection and Control Subcommittee (SPCS) to revise Reliability Standard PRC-019-2;[1]
- Authorize posting of the SAR for a 30-day informal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members.

Background

Reliability Standard PRC-019-2 addresses the reliability issue of miscoordination between generator capability, control systems, and protection functions. However, PRC-019-2 was developed with a bias toward synchronous generation and does not sufficiently outline the requirements for all generation resource types.

The proposed Standard Authorization Request (SAR) aims to address a number of issues identified by the SPCS and revise the standard to be inclusive of all types of generation resources. The SAR was endorsed by the NERC Planning Committee (PC) on March 4, 2020.

Summary

This project proposes revisions to PRC-019-2 to address the following:

- The purpose statement should be inclusive of all generation resource types, including additional clarity in specifying the unique aspects of dispersed power producing resources and reliable coordination of control and protection systems.
- Clarity is needed regarding synchronous generation to remove ambiguity along with updating applicable facilities.
- Requirements need revision to be clear about what must be executed with respect to controllers, momentary cessation, firmware upgrades, and timeframes to perform required coordination.

[1] PRC-019-2 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=PRC-019-2&title=Coordination%20of%20Generating%20Unit%20or%20Plant%20Capabilities,%20Voltage%20Regulating%20Controls,%20and%20Protection&jurisdiction=United%20States

Agenda Item 9a
Standards Committee
January 20, 2021

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to PRC-019 to address dispersed power producing resources		
Date Submitted:	4/7/2020		
SAR Requester			
Name:	Chair Jeffrey Iler & Vice Chair Bill Crossland on behalf of the		
Organization:	NERC System Protection and Control Subcommittee (SPCS)		
Telephone:	Chair: (614) 933-2373 Vice Chair: (216) 503-0613	Email:	Chair: jwiler@aep.com Vice Chair: bill.crossland@rfirst.org
SAR Type (Check as many as apply)			
☒ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☒ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Reliability Standard PRC-019-2 addresses the reliability issue of miscoordination between generator capability, control systems, and protection functions. However, this standard was developed with a bias toward synchronous generation and does not sufficiently outline the requirements for all generation resource types. The purpose statement of the standard requires modification to be inclusive of all generation resource types. While this class of resources are currently included in the applicability of PRC-019-2, additional clarity is needed in specifying the aspects of dispersed power producing resources that should be coordinated. There are also issues within PRC-019-2 regarding synchronous generation that need to be corrected or clarified to remove ambiguity. These comprehensive updates align with the intent and spirit of the standard.			

Requested information

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This project will enhance reliability by maximizing a generators capability and its ability to support grid stability during system disturbances by requiring the coordination of control systems with equipment capabilities and protection functions of all generation resource types.

Project Scope (Define the parameters of the proposed project):

The SDT should develop language that is relevant to all generation resource types. This will include modifications to the purpose statement, the applicability and requirements. Additionally, the SDT should consider modifying Inclusion I4 of the Bulk Electric System (BES) definition and the associated diagrams in the BES Reference Document.

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):

1. **Applicable Facilities** – Clarification of applicable facilities.
   a. Clarify Section 4.2.3.1 to state that it pertains to both the individual resources and the plant level voltage controls. [This section indicates that the individual generating units identified through Inclusion I4 of the Bulk Electric System (BES) definition are included only if voltage control for the facility is performed solely at the individual generator; thus, it is ambiguous as to whether this excludes the individual resources from the standard when the plant/facility level or park controller is being used for voltage control.][2]
   b. Verify that static or dynamic reactive compensating devices (i.e., capacitor banks, static VAR compensators, STATCOMs, etc.) and synchronous condensers within BES generating facilities should be subject to the standard since they must be coordinated for protection and plant capability. [The language in footnote 1[3] for Requirement R1 implies that reactive compensating devices are not applicable since they are not installed or activated on a generator. These devices are system level voltage regulators and have no effect on an individual inverter capability or limiter functions within an inverter control system; however, they are important to system VAR support and reliability. For example, Type 1 and Type 2 wind turbine generators (WTG) typically employ reactive compensating devices on the collector side of the generator step-up (GSU) transformer. In this case, reactive compensating devices are integral to supporting the systems reactive needs and enhances the reliability of the BES. These devices are not captured by the BES definition because they typically connect at voltages less than 100 kV; however, they should be applicable to the standard for asynchronous and non-rotating resources.]

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Reference Section 4.10.10 of the White Paper from Project 2014-01 Standards Applicability for Dispersed Generation Resources

[3] "Limiters or protection functions that are installed and activated on the generator or synchronous condenser."

Requested information

c. Revise Inclusion I4 of the BES definition and Figures I4-1, I4-2, I4-3, and I4-4 in the BES Reference Document to accurately depict all generation resources.

2. **Requirement(s)** – Ensure the language is clear and inclusive of all generation resource types with respect to coordinating control systems, protection functions, and equipment capabilities.

d. **Controllers specific to dispersed power producing resources** – The standard is currently biased toward automatic voltage regulating (AVR) control systems used in conjunction with synchronous generation. The standard should address other control systems associated with dispersed power producing resources that are essential to reliability. Typically, inverters have a control system and the facility has a plant controller with a separate control system. The inverter has a control system that may operate in VAR control, Power Factor control, reactive power priority, or active power priority. The plant controller has a control system that may operate in Power Factor or Voltage Control modes. Coordination between any plant/park controller with individual resource control systems must be achieved to prevent unnecessary reduction of the resource.

e. **Momentary cessation** – "Momentary cessation" is a function within an Inverter-Based Resource (IBR) control system that reduces active and reactive current to zero when voltage is outside of a defined band.[4] A reduction in active and/or reactive current can negatively impact reliability, especially during system perturbations, since the function prohibits the IBR from providing support to the BPS during these events.[5] Ensuring clear language in this standard will ensure that BES generators are not unnecessarily ceasing current injection during abnormal conditions, that any cessation of current is coordinated with equipment capability, and that these functions do not pose a risk to BPS reliability.[6] Revisions to the standard should consider methods or parameters to eliminate momentary cessation where possible, otherwise ensure it is coordinated with equipment capabilities of the inverter where it cannot be eliminated (for legacy equipment).

f. **Controller upgrades and/or changes (e.g., firmware)** – Specify that firmware upgrades are considered "system, equipment or setting changes" under Requirement R2 since these may impact dispersed power producing resource voltage control(s), protection, and limiters.

g. **Steady State Stability Limit (SSSL)** – Determine whether the "stability limits" language in Requirement R1.1.2 should be removed from the standard. [Manual SSSL theory is only applicable when a generator AVR is in manual operation mode; however, the standard specifically instructs an entity to assume the AVR is in automatic mode. This assumption is identified because it is industry standard to coordinate the underexcitation limiter with the SSSL since that is the most conservative approach for AVR operation. However, the

[4] The voltage settings that cause momentary cessation are considered voltage protection settings within the inverter. Other functions within the inverter can cause momentary cessation to operate in a manner similar to a protective function. However, the focus for PRC-019 is on voltage-related functions.

[5] Including dynamic active power-frequency control and reactive power-voltage control.

[6] Momentary cessation has been observed in BPS solar PV facilities in all disturbances analyzed by NERC, including but not limited to the Blue Cut Fire, Canyon 2 Fire, Palmdale Roost, and Angeles Forest disturbances.

Requested information
protection settings typically coordinate with the machine capabilities and not the manual SSSL.] h. **Synchronous condensers** – If item 'd' remains in the standard, determine whether SSSL should be considered for synchronous condensers. [A synchronous condenser operates in a manner similar to a synchronous generator in terms of voltage regulation and the associated excitation control system. The electrical quantities for a synchronous condenser match the quantities specified in the manual SSSL methodology; however, the machine does not have a prime mover and cannot output real power. This drastically reduces the machines operating region since the unit will only be able to absorb or generate reactive power.] i. **Stability limits for other types of generation resources** – If item 'd' remains in the standard, verify whether a SSSL must be considered for asynchronous and non-rotating generation resources. [Current references to stability limits are all relevant to synchronous machines (AVR in manual mode, fixed excitation voltage, etc.). If consideration of stability is necessary, provide a methodology or implementation guidance for the industry to use (e.g. small signal stability, etc.)]. j. **Voltage drop across dispersed power producing resource collector system** – Determine whether the voltage drop across the collector system, bus, generator step-up (GSU) transformer, or other facilities should be considered for coordination. k. **Time frame to perform coordination** – Revise the language in Requirement R2 to remove ambiguity surrounding the timeframe for performing coordination. [The current language can be interpreted as allowing the coordination to be performed 90 days after the "implementation of systems, equipment, or setting changes." This would allow an entity to put a unit back into service without performing coordination; thus, jeopardizing reliability. The original SDT has confirmed that the 90-day time frame was for scenarios in which an entity discovered a miscoordination.]
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Costs may include updating firmware on dispersed power producing resources, individual IBRs, park/plant controllers, and other associated equipment, and will vary depending on the approach taken to address the reliability-related risks stated above.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Synchronous generation and dispersed power producing resources may be impacted by the revisions.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
The team should be made up predominantly by protection engineers with a background in generation protection (synchronous/dispersed power producing resources); preferably industry experts in this field. Additionally, IBR manufacturers and Engineering, Procurement and Construction firms familiar with

Requested information
dispersed power producing resources should be included because of their inherent knowledge of the capabilities and limitations of dispersed power producing resources. Team members should have extensive understanding of generation protection concepts/schemes. In addition, they should have some knowledge of control systems (AVR, IBR's, etc.)
Do you know of any consensus building activities[7] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
No
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The NERC SPCS initially attempted to develop Implementation Guidance (IG); however, while developing the IG, the group determined that the standard required additional clarity for IBRs.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

[7] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 10
Standards Committee
January 20, 2021

Standard Authorization Request
Transmission Relay Loadability

Action

- Accept the Standard Authorization Request (SAR) that was submitted by the System Protection and Control Working Group proposing to revise NERC Reliability Standard PRC-023-4;[1]
- Authorize posting of the SAR for a 30-day informal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members.

Background

PRC-023-4, Requirement R2 requires applicable functional entities to set their Out of Step Blocking[2] (OOSB) elements to allow tripping for faults during the loading conditions prescribed by Requirement R1. A requirement to allow tripping in a Standard whose intent is to block tripping, has led to some functional entities disabling their OOSB relays. Disabling of these relays increases the possibility of unnecessary tripping during a stable power swing and posing increased risk to reliability. OOSB relays provide increased security by preventing relays from tripping for stable power swings. Preventing the tripping of transmission lines during power swings increases the reliability of the BES.

Requirement R2 has also been interpreted to restrict the setting of OOSB elements making compliance with PRC-026-1 (Relay Performance During Stable Power Swings) more difficult.

Summary

The project proposes to improve the current PRC-023-4 standard by retiring Requirement R2 that mandates tripping for faults when Requirement R1 already requires functional entities to provide “reliable protection [i.e., tripping] of the BES for all fault conditions.” Also retiring Attachment A exclusion 2.3 removes the perceived restriction for setting OOSB relays and enhances the ability to apply OOSB relays in PRC-026-1.

[1] PRC-023-4, Transmission Relay Loadability, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=PRC-023-4&title=Transmission%20Relay%20Loadability&jurisdiction=United%20States

[2] The term power swing blocking (PSB) is also used by industry to describe these elements.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda Item 10a
Standards Committee
January 20, 2021

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to PRC-023-4		
Date Submitted:	October 19, 2020		
SAR Requester			
Name:	Jeff Iler, Chair & Bill Crossland, Vice Chair (on behalf of)		
Organization:	NERC System Protection and Control Working Group		
Telephone:	Jeff: (614) 933-2373 Bill: (216) 503-0600	Email:	Jeff: jwiler@aep.com Bill: bill.crossland@rfirst.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Requirement R2, in PRC-023-4, requires applicable functional entities to set their Out of Step Blocking[1] (OOSB) elements to allow tripping for faults during the loading conditions prescribed by Requirement R1. A requirement to allow tripping in a Standard whose intent is to block tripping, has led to some entities disabling their OOSB relays. Disabling of these relays could lead to tripping during stable power swings causing an increased reliability risk. OOSB relays provide increased security by preventing relays from tripping for stable power swings. Preventing the tripping of transmission lines during these types of disturbances increases the reliability of the BES. Requirement R2 should be removed because it has been interpreted to restrict the setting of OOSB elements making compliance with PRC-026 more difficult. Attachment A exclusion 2.3 should also be removed. This exclusion is no longer needed and that exclusion has contributed to the confusion surrounding R2. Attachment A exclusion 2.3 has been			

[1] The term power swing blocking (PSB) is also used by industry to describe these elements

Requested information
interpreted as being in conflict with R2. Both R2 and Attachment A exclusion 2.3 are not needed in the Standard.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The purpose of the proposed project provides a reliability-related benefit by eliminating PRC-023-4 Requirement R2. This will eliminate entities disabling their OOSB elements unnecessarily. It will remove an unnecessary exclusion (Attachment A – 2.3) for relays that no longer need an exclusion.
Project Scope (Define the parameters of the proposed project):
The scope includes: • Retire Requirement R2. • Remove Attachment A, Item 2.3 exclusion with regard to the use of protection systems during stable power swings. • Make comporting changes to the standard as needed to address the retirement of Requirement R2 and to remove Attachment A, Item 2.3 exclusion. • Ensure that removing the Item 2.3 exclusion does not overlap or create a gap with intent of PRC-026 – Relay Performance During Stable Power Swings. • Making any administrative non-substantive corrections. • Modify the Supplemental Technical Reference Document, "Determination and Application of Practical Relaying Loadability Ratings Version 1", referenced in PRC-023-4, as needed to address the retirements and removal. Specifically, the Out of Step Blocking section.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[2] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
The PRC-023 standard is about setting protective relays so they do not limit transmission loadability, meaning they do not trip unnecessarily during heavy loading conditions while still being capable of detecting all fault conditions.[3] The intent of Requirement R2 is to ensure out-of-step blocking (OOSB) elements allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability. Requirement R2 is about ensuring OOSB elements allow blocked relay elements to trip reliably (i.e., if a three-phase fault occurs while OOSB is asserted) and not about ensuring protection systems do not limit transmission loadability. OOSB elements differentiate between power swings and three-phase faults. During a power swing, an OOSB element will typically block phase distance elements (i.e., Zone 1 & Zone 2 phase distance elements) from tripping. According

[2] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[3] PRC-023-4, Purpose: "Protective relay settings shall not limit transmission loadability; not interfere with system operators' ability to take remedial action to protect system reliability and; be set to reliably detect all fault conditions and protect the electrical network from these faults."

Requested information

to Requirement R2, an OOSB element must unblock the blocked phase distance elements for faults that occur during the loading conditions used to set the protective relay under Requirement R1. Also in the standard, Attachment A, Item 2.3 excludes protection systems intended for protection during stable power swings and is seen as contradictory with Requirement R2 because these protection systems are associated with the use of OOSB elements, whose primary purpose is to ensure phase distance elements don't trip during stable power swings.

The apparent intent of Requirement R2 is to ensure that OOSB elements don't pick up, time out, and block distance elements from tripping for three-phase faults during the loading conditions described in Requirement R1. The protection engineer must ensure reliable fault protection and has various tools in modern microprocessor based relays to ensure the dependable unblocking of tripping elements during faults. Applying the loadability criteria while ensuring reliable fault protection is already an underpinning of Requirement R1.[4] For example, an engineer can apply the use of override timers[5] that are available in modern microprocessor relays or can add such timers to existing electromechanical relay elements. An engineer can also use advanced microprocessor-based zero-setting OOSB algorithms. Applying the loadability criteria to relay settings under Requirement R1 somewhat meets the intent of Requirement R2 because Requirement R1 mandates not limiting transmission loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. Additionally, Requirement R2 restrictively dictates the boundary setting of the OOSB element that starts the OOSB timer which has the overall effect of reducing the slip rate for which the OOSB element will correctly block. This results in decreasing the security of the protection scheme and increasing the chance that a misoperation of a distance element will occur for power swings that are faster than the allowable slip rate. Requirement R2 also impacts the ability to comply with NERC Reliability Standard PRC-026 (Relay Performance During Stable Power Swings) in that it affects the application of OOSB relaying that is integral to the purpose of PRC-026, which is "[t]o ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions".

Attachment A, 2.3 was included for protection systems that intentionally trip during power swing disturbances, such as intentional islanding schemes. Florida was cited as an example of where these schemes were employed. Research has indicated that these schemes no longer exist and there is no need for a power swing tripping exclusion.

Requirement R2 was added to PRC-023 in version 2 after filing version 1 with FERC.[6] FERC observed that Attachment A item 2 in PRC-023-1 was a requirement and that it needed to be included in the requirements section of a standard with the appropriate violation risk factors and violation severity levels.

[4] PRC-023-4, "R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability **while maintaining reliable protection of the BES for all fault conditions**. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees."

[5] OOSB relays with override timers will allow the OOSB blinder that starts the timer to be set beyond the loadability region prescribed by the standard. The OOSB relay would unblock after a predetermined delay should an unlikely three-phase fault occur.

[6] See FERC Order 733 para 244 https://www.ferc.gov/whats-new/comm-meet/2010/031810/E-5.pdf

Requested information
The original SDT included the "warning" in Attachment A item 2, with regards to OOSB, in reference to the OOSB timer. Some OOSB schemes employ an outer and an inner impedance blinder with a timer that is used to determine the rate of change of apparent impedance to differentiate between a fault (fast change) and a swing (slow change). The timer starts timing when the impedance passes through (is less than) the outer blinder. If the impedance does not pass through the inner blinder (is less than), before the timer setting, the OOSB will declare a swing and block the phase distance elements from tripping. The SDT wanted to inform entities that they could experience loading conditions that would result in an impedance that was between the OOSB blinders for a long period of time that would result in the blocking of the phase tripping elements indefinitely. This condition could exist at any time regardless of a relay loadability requirement. Therefore, this should not be a requirement associated with PRC-023. It is good engineering practice to ensure your relays will operate properly for all conditions they are expected to experience. This should not be a requirement in a relay loadability Standard. OOSB elements are included in the Relay Performance During Stable Power Swings Standard PRC-026-1. PRC-026-1 already includes the language "while maintaining dependable fault detection" in regards to OOSB supervision. Attachment A item 2.3 excludes "Protection systems intended for protection during stable power swings". This exclusion is referencing "Protection systems installed specifically to separate portions of the system that are experiencing stable power swings relative to each other in order to maintain desirable performance relative to voltage, frequency, and power oscillations"[7]. These Out of Step Tripping (OOST) protection systems are better addressed in the standard for power swings, PRC-026.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Should reduce cost to Registered Entities by eliminating the compliance monitoring of a requirement that is addressed by another standard. Revising the exemption should not have a significant impact on cost.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
Transmission facilities that use OOSB functionality and that experience significant oscillations (i.e., power swings) has the benefit of ensuring the system remains intact where separation of portions of the transmission system could occur due to power swings.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Transmission Owner, Generator Owner, and Distribution Provider

[7] See Project 2010-13.1 Phase 1 of Relay Loadability: Transmission Draft 1 Relay Loadability Standard Consideration of Comments https://www.nerc.com/pa/Stand/Project%202010131%20Phase%201%20of%20Relay%20Loadability%20Trans/Consider_Comments_1st_Draft_Relay_Loadability_Std_09Jan07.pdf

Requested information
Do you know of any consensus building activities[8] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
N/A
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
PRC-026 – Relay Performance During Stable Power Swings (Note: Project 2015-09 – Establish and Communicate System Operating Limits is proposing modifications to PRC-026 due to revisions to the definition of System Operating Limit).
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
N/A

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes

[8] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
N/A	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

Agenda Item 11
Standards Committee
January 20, 2021

Standard Authorization Request
Disturbance Monitoring and Reporting Requirements

Action

- Accept the Standard Authorization Request (SAR) submitted by the NERC Inverter-Based Resource Performance Task Force (IRPTF) to modify Reliability Standard PRC-002-2;[1]
- Authorize posting of the SAR for a 30-day informal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members.

Background

The purpose of PRC-002-2 is to have adequate data available to facilitate analysis of Bulk Electric System (BES) disturbances. The standard has a methodology which determines locations for capturing Sequence of Events Recording (SER), fault recording (FR) Data, and dynamic disturbance recording (DDR) data on BES elements with short circuit MVA in the top 20%. Hence, synchronous generator dominated systems that contribute significantly to the short circuit MVA calculation heavily influence the location of data recording. In contrast, asynchronous generators (i.e., inverter-based resources (IBRs)) do not contribute a significant level of short circuit current and are usually interconnected in parts of the system remote to synchronous machines. As such, their short circuit MVA generally does not reach the top 20% and they are more likely to be omitted from requiring SER and FR data monitoring. In addition, most IBRs do not meet the nameplate rating criteria for inclusion to have DDR.

With increasing penetration of IBRs, it is important that some of these resources and nearby BES elements are monitored with SER, FR and DDR devices. For example, recent disturbance analyses of events involving IBRs including the Blue Cut Fire and Canyon 2 Fire have demonstrated the lack of disturbance monitoring data available from these facilities and nearby BES buses to adequately determine the causes and effects of their behavior.

The IRPTF undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The "IRPTF Review of NERC Reliability Standards White Paper"[2] was approved by the Operating Committee and the Planning Committee in March 2020. Additionally, the IRPTF produced "BPS-Connected Inverter-Based Resource Performance"[3] (see Chapter 6) and

[1] PRC-002-2 Disturbance Monitoring and Reporting Requirements, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=PRC-002-2&title=Disturbance%20Monitoring%20and%20Reporting%20Requirements&jurisdiction=United%20States

[2] IRPTF Review of NERC Reliability Standards, NERC Inverter-Based Resource Performance Task Force (IRPTF) White Paper - March 2020, https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/Review_of_NERC_Reliability_Standards_White_Paper.pdf

[3] Reliability Guideline – BPS-Connected Inverter-Based Resource Performance, September 2018, https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf

"Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources"[4] reliability guidelines touch on monitoring considerations for IBRs.

The Reliability, Security, and Technology Committee (RSTC) endorsed the SAR on June 10, 2020.

Summary

This SAR proposes to revise PRC-002-2 to address gaps within the existing standard. The goal is to modify the requirements to ensure adequate data is available and periodically assessed to facilitate the analysis of BES disturbances, including in areas of the Bulk Power System (BPS) that may not be covered by the existing requirements. The proposed scope of this project is as follows:

- Consider ways to ensure that the identification and periodic assessment of BES and/or BPS buses for which SER and FR data is required provides adequate monitoring of BES Disturbances. This may include updates to supplemental information such as the previously provided "Median Method Excel Workbook".
- Consider ways to ensure that the identification and periodic assessment of BES and/or BPS Elements for which DDR data is required provides adequate monitoring of BES disturbances.
- Consider other manners in which to add to, modify or clarify the existing requirements to ensure adequate monitoring of BES disturbances.

[4] NERC Reliability Guideline – Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources, September 2019, https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda Item 11a
Standards Committee
January 20, 2021

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	PRC-002-2 Disturbance Monitoring and Reporting Requirements		
Date Submitted:	June 10, 2020		
SAR Requester			
Name:	Allen Shriver, Chair Jeffery Billo, Vice Chair		
Organization:	Inverter-Based Resource Performance Task Force (IRPTF)		
Telephone:	Allen: 561-904-3234 Jeffery: 512-248-6334	Email:	Allen.Schriver@NextEraEnergy.com Jeff.Billo@ercot.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The NERC Inverter-based Resource Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements based on the work and findings of the IRPTF. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The “IRPTF Review of NERC Reliability Standards White Paper” was approved by the Operating Committee and the Planning Committee in March 2020. Among the findings noted in the white paper, the IRPTF identified issues with PRC-002-2 that should be addressed. The purpose of PRC-002-2 is to have adequate data available to facilitate analysis of BES disturbances. Requirements R1 and R5 specify where sequence of events recording (SER) and fault recording (FR) data, and where dynamic Disturbance recording (DDR) data, respectively, are required in the Bulk Electric System (BES).			

Requested information

Requirements R1 and R5 are written with a focus on synchronous machine dominated systems with periodic review of monitoring equipment needs for the system. The BES elements with short circuit MVA in the top 20% are typically elements at baseload generating plants with multiple generating units or BES elements within a heavily meshed transmission network usually close to large load centers. Inverter-based resources (IBRs) do not contribute much fault current and are usually interconnected in remote parts of the system. As such, the short circuit MVA for the point of interconnection (POI) bus and nearby BES buses is not expected to be in the top 20%. Hence, BES buses near these resources are more likely to be omitted from requiring SER and FR data monitoring. In addition, most IBRs do not meet the nameplate rating criteria outlined in Requirement R5. With increasing penetration of IBRs, it is important that some of these resources and nearby BES elements are monitored with DDR and SER/FR devices.

Recent disturbance analyses of events involving IBRs including the Blue Cut Fire and Canyon 2 Fire have demonstrated the lack of disturbance monitoring data available from these facilities and nearby BES buses to adequately determine the causes and effects of their behavior. None of the IBRs involved in these two events met the size criteria stated in PRC-002-2 to be required to have disturbance monitoring. Additionally, none of the buses near the IBRs met the criteria in Requirement R1 for being required to have SER and FR devices since the IBRs inherently produce very little fault current. This led to difficulty in adequately assessing the events.

With the changing resource mix and increasing penetration of IBRs, PRC-002-2 does not serve its intended purpose adequately. To the extent that the standard is already requiring monitoring devices and periodic assessments, the location requirements and associated periodic assessments need to be revised. These revisions are necessary so that required data is available for the purposes of post-mortem event analysis and identifying root causes of large system disturbances.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This SAR proposes to revise PRC-002-2 to address gaps within the existing standard. The goal is to modify the requirements to ensure adequate data is available and periodically assessed to facilitate the analysis of BES disturbances, including in areas of the Bulk Power System (BPS) that may not be covered by the existing requirements.

Project Scope (Define the parameters of the proposed project):

The proposed scope of this project is as follows:

a. Consider ways to ensure that the identification and periodic assessment of BES and/or BPS buses for which SER and FR data is required provides adequate monitoring of BES Disturbances. This may include updates to supplemental information such as the previously provided “Median Method Excel Workbook”.

b. Consider ways to ensure that the identification and periodic assessment of BES and/or BPS Elements for which DDR data is required provides adequate monitoring of BES disturbances.

Requested information

c. Consider other manners in which to add to, modify or clarify the existing requirements to ensure adequate monitoring of BES disturbances.

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):

Per Requirement R1 (which uses criteria outlined in Attachment 1), Sequence of Event Recording (SER) and Fault Recording (FR) devices are required at BES buses with high short circuit MVA values. The methodology identifies the top 20 percent of BES buses with highest short circuit MVA values and requires a subset of these buses to be monitored for SER and FR data.

However, BES elements with short circuit MVA in the top 20% are typically elements at baseload generating plants with multiple generating units or BES elements within a heavily meshed transmission network usually close to large load centers. IBRs do not contribute much fault current and are usually interconnected in remote parts of the system. As such, the short circuit MVA for the point of interconnection (POI) bus and nearby BES buses is not expected to be in the top 20%. Hence, BES buses near these resources are more likely to be omitted from requiring SER and FR data monitoring, though it is possible that monitoring in these areas is needed for disturbance analysis, as was the case in the Blue Cut Fire and Canyon 2 Fire events.

Requirement R5, identifies BES locations based on a size criteria for generating resources and other critical elements such as HVDC, IROLs and elements of UVLS program, for which Dynamic Disturbance Recording (DDR) data is required. In regard to generation resources, it includes requirements for monitoring at sites with either gross individual nameplate rating of greater than or equal to 500 MVA or gross individual nameplate rating greater than or equal to 300 MVA where gross plant/facility aggregate nameplate rating is greater than or equal to 1000 MVA.

However, most IBRs do not meet the nameplate rating criteria outlined in Requirement R5. With increasing penetration of IBRs, it is important that some of these resources and nearby BES elements are monitored with DDR devices to ensure adequate coverage for disturbance analysis while balancing cost impacts.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

The SAR proposes to modify PRC-002-2 requirements. The cost impact is unknown, however, the cost of disturbance monitoring hardware is approximately $50,000 to $100,000 per installation if the existing onsite equipment is not already set up for monitoring and storage.

Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
IBRs contribute very little short circuit MVA and are typically smaller in aggregate nameplate rating when compared to legacy synchronous resources. The criteria for selecting disturbance monitoring locations should take this into account.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Planning Coordinator, Reliability Coordinator, Generator Owner, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This issue was captured in the "IRPTF Review of NERC Reliability Standards White Paper" which was approved by the Operating Committee and the Planning Committee. Additionally, the IRPTF produced "BPS-Connected Inverter-Based Resource Performance"(see Chapter 6) and "Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources" reliability guidelines touch on monitoring considerations for IBRs.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
N/A
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The IRPTF did not identify any alternatives since there is a gap in PRC-002-2.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
□	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
□	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 12
Standards Committee
January 20, 2021

Standard Authorization Request
Generator Operation for Maintaining Network Voltage Schedules

Action

- Accept the Standard Authorization Request (SAR) submitted by the Inverter-Based Resource Performance Task Force (IRPTF) to revise Reliability Standard VAR-002-4.1, Requirement R3;[1]
- Authorize posting of the SAR for a 30-day informal comment period; and
- Authorize for solicitation of SAR Drafting Team (DT) members

Background

Reliability Standard VAR-002-4.1 requires, among other things, Generator Operators (GOP) to ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection. For dispersed power producing resources, it is not clear if a GOP is required to notify the Transmission Operator (TOP) for the status change of a voltage controlling device on an individual generating unit within a Facility comprised of numerous resources. NERC Project 2014-01 Standards Applicability for Dispersed Generation Resources revised VAR-002, Requirement R4, to clarify that it is not applicable to individual generating units of dispersed power producing resources. At the time, the IRPTF did not identify any reason why Requirement R3 (i.e., “status change”) should be treated differently than Requirement R4.

The NERC IRPTF undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper[2] approved by the Operating Committee. Among the findings noted in the white paper, the IRPTF identified issues with VAR-002-4.1 that should be addressed through the standards development process.

The SAR was endorsed by the Reliability, Security, and Technology Committee (RSTC) on June 10, 2020.

Summary

The proposed scope of this project is to clarify VAR-002-4.1, Requirement R3, in regards to whether the GOP of a dispersed power resource must notify its associated TOP upon a status change of a voltage controlling device on an individual generating unit; for example, if a single inverter goes offline in a solar photo-voltaic (PV) Facility.

[1] VAR-002-4.1 - Generator Operation for Maintaining Network Voltage Schedules, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=VAR-002-4.1&title=Generator%20Operation%20for%20Maintaining%20Network%20Voltage%20Schedules&jurisdiction=United%20States

[2] IRPTF Review of NERC Reliability Standards White Paper, March 2020approved by the Operating Committee and the Planning Committee in March 2020, https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/Review_of_NERC_Reliability_Standards_White_Paper.pdf

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information	
SAR Title:	VAR-002-4.1 Generator Operation for Maintaining Network Voltage Schedules
Date Submitted:	June 10, 2020

SAR Requester

Name:	Allen Shriver, Chair Jeffery Billo, Vice Chair		
Organization:	Inverter-Based Resource Performance Task Force (IRPTF)		
Telephone:	Allen: 561-904-3234 Jeffery: 512-248-6334	Email:	Allen.Schriver@NextEraEnergy.com Jeff.Billo@ercot.com

SAR Type (Check as many as apply)

□ New Standard	□ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	
□ Add, Modify or Retire a Glossary Term	□ Variance development or revision
□ Withdraw/retire an Existing Standard	□ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

□ Regulatory Initiation	☒ NERC Standing Committee Identified
□ Emerging Risk (Reliability Issues Steering Committee) Identified	□ Enhanced Periodic Review Initiated
□ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The NERC Inverter-based Resource Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or improvements based on the work and findings of the IRPTF. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in a white paper. The "IRPTF Review of NERC Reliability Standards White Paper" was approved by the Operating Committee and the Planning Committee in March 2020. Among the findings noted in the white paper, the IRPTF identified issues with VAR-002-4.1 that should be addressed.

The purpose of VAR-002-4.1 is "to ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection." Requirement R3 requires each Generator Operator (GOP) to notify its

Requested information
Transmission Operator (TOP) of a status change on “the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change.” Requirement R4 is similar in that it requires each GOP to notify its TOP of “a change in reactive capability due to factors other than a status change described in Requirement R3.” For dispersed power producing resources, it is not clear if a GOP is required to notify the TOP for the status change of a voltage controlling device on an individual generating unit. For example, if an IBR consisting of one hundred inverters has one inverter trip out of service, is the GOP required to notify the TOP per Requirement R3? NERC Project 2014-01 revised VAR-002 Requirement R4 to clarify that it is not applicable to individual generating units of dispersed power producing resources. The IRPTF did not identify any reason why Requirement R3 should be treated differently than Requirement R4 in this respect and recommended VAR-002-4.1 be modified to make this same clarification to Requirement R3.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This SAR proposes to revise VAR-002-4.1 to address ambiguities within the existing standard. The goal is to add clarity and address the ambiguity in the existing requirements.
Project Scope (Define the parameters of the proposed project):
The proposed scope of this project is to clarify VAR-002-4.1 Requirement R3 in regards to whether the GOP of a dispersed power resource must notify its associated TOP of a status change of a voltage controlling device on an individual generating unit, for example if a single inverter goes offline in a solar PV resource.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
The Standards Drafting Team should clarify VAR-002-4.1 Requirement R3 in regards to whether the GOP of a dispersed power resource must notify its associated TOP of a status change of a voltage controlling device on an individual generating unit.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The SAR proposes to clarify VAR-002-4.1 Requirement R3. The cost impact is unknown, but it is expected to be minimal since it should only impact communication procedures.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Dispersed power producing resources are made up of multiple individual generating units. It may be impractical, place an undue burden upon the associated GOPs and TOPs, and have no material reliability benefit to have GOPs notify TOPs in regards to the status change of a voltage controlling device on a single individual generating unit.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Generator Operators and Generator Owners
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This issue was captured in the "IRPTF Review of NERC Reliability Standards White Paper" which was approved by the Operating Committee and the Planning Committee.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
N/A
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
The IRPTF did not identify any alternatives since the language in VAR-002-4.1 needs clarification.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

□ Draft SAR reviewed by NERC Staff
□ Draft SAR presented to SC for acceptance
□ DRAFT SAR approved for posting by the SC

□ Final SAR endorsed by the SC
□ SAR assigned a Standards Project by NERC
□ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 13
Standards Committee
January 20, 2021

NERC Legal and Regulatory Update

November 26, 2020 – January 4, 2021

NERC FILINGS TO FERC SUBMITTED SINCE LAST SC UPDATE

FERC Docket No.	Filing Description	FERC Submittal Date
RM13-11-000	2020 Frequency Response Annual Analysis Report NERC submitted its 2020 Frequency Response Annual Analysis report for the administration and support of Reliability Standard BAL-003-2 – Frequency Response and Frequency Bias Setting.	12/1/2020
RM05-17-000, RM05-25-000, RM06-16-000	2021-2023 Reliability Standards Development Plan NERC submitted its Reliability Standards Development Plan (RSDP) for 2021-2023. This informational filing provides a status update on active development projects and a forecast of future work to be undertaken by NERC and its stakeholders throughout the upcoming year.	12/8/2020
RD21-2-000	NERC Petition for Approval of Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 NERC submitted its petition for approval of proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 addressing supply chain cybersecurity risk management.	12/14/2020
EL21-13-000	Joint Answer to the Amended Complaint NERC and WECC submitted a Joint Answer to the Amended Complaint by Californians for Green Nuclear Power, Inc.	12/15/2020
RD20-2-000	CIP SDT Schedule December Update Informational Filing NERC submitted to FERC an informational compliance filing as directed by FERC in its February 20, 2020 Order. This filing contains a status update on two standards development projects relating to CIP Reliability Standards.	12/15/2020

RM19-20-000	Joint Comments on BAL-002-WECC-3 NOPR NERC and WECC submitted joint comments on the Commission's Notice of Proposed Rulemaking regarding proposed Reliability Standard BAL-002-WECC-3.	12/18/2020

FERC ISSUANCES SINCE LAST SC UPDATE

FERC Docket No.	Issuance Description	FERC Issuance Date
RM20-8-000	FERC Order Directing Informational Filing Regarding Virtualization and Cloud Computing Services FERC issued an order directing NERC to begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner and to make an informational filing by January 1, 2022.	12/17/2020
RD21-1-000	Letter order approving reliability standard PRC-006-5 FERC issued a letter order approving proposed Reliability Standard PRC-006-5.	12/23/2020
RR20-5-000	Order conditionally approving a revised pro forma Delegation Agreement; and revised RDAs between NERC and each of the six Regional Entities FERC issued an order conditionally approving a revised pro forma Delegation Agreement; and revised delegation agreements between NERC and each of the six Regional Entities (RDAs).	12/30/2020

ANTICIPATED UPCOMING FILINGS

FERC Docket No.	Filing Description	Anticipated Filing Date
RD21-3-000	FAC-001-3 errata	1/7/2021
TBD	Petition for Approval of SERC RSDP	TBD

Standards Committee Expectations

Approved by Standards Committee January 12, 2012

Background

Standards Committee (SC) members are elected by members of their segment of the Registered Ballot Body, to help the SC fulfill its purpose. According to the Standards Committee Charter, the SC's purpose is:

> *In compliance with the NERC Reliability Standards Development Procedure, the Standards Committee manages the NERC standards development process for the North American-wide reliability standards with the support of the NERC staff to achieve broad bulk power system reliability goals for the industry. The Standards Committee protects the integrity and credibility of the standards development process.*

The purpose of this document is to outline the key considerations that each member of the SC must make in fulfilling his or her duties. Each member is accountable to the members of the Segment that elected them, other members of the SC, and the NERC Board of Trustees for carrying out their responsibilities in accordance with this document.

Expectations of Standards Committee Members

1. SC members represent their segment, not their organization or personal views. Each member is expected to identify and use mechanisms for being in contact with members of the segment in order to maintain a current perspective of the views, concerns, and input from that segment. NERC can provide mechanisms to support communications if an SC member requests such assistance.

2. SC members base their decisions on what is best for reliability and must consider not only what is best for their segment, but also what is in the best interest of the broader industry and reliability.

3. SC members should make every effort to attend scheduled meetings, and when not available are required to identify and brief a proxy from the same segment. SC business cannot be conducted in the absence of a quorum, and it is essential that each SC member make a commitment to being present.

4. SC members should not leverage or attempt to leverage their position on the SC to influence the outcome of standards projects.

5. The role of the SC is to manage the standards process and the quality of the output, not the technical content of standards.

Agenda Item 14d
Standards Committee
January 20, 2021

Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 11th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." The vote is subject to a 2/3 majority approval. Also, any member may call the question. This motion is not debatable. The vote is subject to a 2/3 vote.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The “seconder” is not recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee “owns” the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent The standard practice.	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.