NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

December 18, 2019 | 10:00 a.m. — 3:00 p.m. Eastern

Dial-in: 1-415-655-0002 | Access Code: 734 884 657 | Meeting Password: 121819
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 December 18 Agenda — Approve** (A. Gallo) (1 minute)
2. **Consent Agenda** (A. Gallo) (5 minutes)
   a. November 20, 2019 Standards Committee Meeting Minutes* **— Approve**
   b. 2020-2022 SC Strategic Work Plan* **— Approve**
   c. 2019 Annual Accomplishments* **— Endorse**
3. **Projects Under Development — Review**
   a. Three-month Outlook* (H. Gugel) (10 minutes)
   b. Project Tracking Spreadsheet (C. Yeung) (5 minutes)
   c. Projected Posting Schedule (H. Gugel) (5 minutes)
4. **Project 2019-02 BES Cyber System Information Access Management* — Authorize** (S. Kim) (15 minutes)
5. **Project 2019-05 Modifications to PER-003-2* — Accept / Authorize / Appoint** (S. Kim) (15 minutes)
6. **Project 2019-06 Cold Weather SAR Drafting Team* CONFIDENTIAL — Appoint** (S. Kim) (15 minutes)
7. **Project 2015-09 System Operating Limits* — Appoint** (S. Kim) (5 minutes)
8. **BAL-003-2 Errata* — Approve** (S. Kim) (10 minutes)
9. **Standards Efficiency Review Evidence Retention* — Endorse** (M. Puscas) (15 minutes)
10. **Project 2019-04 Modifications to PRC-005-6 SAR DT* — Reconsider CONFIDENTIAL** (A. Gallo) (15 minutes)

11. **Drafting Team Nominee Selection* — Discuss (J. Flandermeyer) (15 minutes)**
12. **Subcommittee Reports — Update**
    a. Project Management and Oversight Subcommittee (PMOS)* — (C. Yeung) (15 minutes)
    b. Standards Committee Process Subcommittee (SCPS) — (S. Bodkin) (15 minutes)
13. **Legal Update and Upcoming Standards Filings* — Review** (L. Perotti) (5 minutes)
14. **Informational Items — Enclosed**
    a. SCEC Election*
    b. SC Special Election*
    c. Standards Committee Expectations*
    d. 2020 SC Meeting Schedule
    e. 2019 Standards Committee Roster
    f. 2020 Standards Committee Roster
    g. Highlights of Parliamentary Procedure*
15. **Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Announcement

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

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

Participants are reminded that 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 Meeting
November 20, 2019 | 1:00 – 3:00 p.m. Eastern

A. Gallo, chair, called to order the meeting of the Standards Committee (SC or the Committee) on November 20, 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 Mendonca.

Introduction and Chair's Remarks
A. Gallo welcomed the Committee and guests, and acknowledged the people attending as proxies.

Review November 20, 2019 Agenda (agenda item 1)
The Committee approved the November 20, 2019 meeting agenda by unanimous consent.

Consent Agenda (agenda item 2a)
The Committee approved the October 23, 2019 SC meeting minutes by unanimous consent.

Projects Under Development (agenda item 3)
C. Yeung reviewed the Project Tracking Spreadsheet. He highlighted relevant information for each project. S. Kim reviewed the Projected Posting Schedule.

2020-2022 Strategic Work Plan (agenda item 4)
A. Gallo stated a new SC Work Plan has been drafted and will be sent to SC members for comment due by December 2.

Project 2015-09 Establish and Communicate System Operating Limits (agenda item 5)
S. Kim and Project 2015-09 standard drafting team (SDT) members provided an update as summarized in the one-pager. The SDT recently discussed newly proposed standards language in FAC-011 that would address concerns raised by FERC staff. S. Bodkin asked for more clarification about the SOL data FERC had requested and SDT response. H. Gugel and the SDT chair stated, as described in the one-pager, the data was inconsistent, since the entities used different tools to collect and store. The SDT believed additional data would take a year or more to collect. The SDT is planning an informational webinar to share the revised FAC-011 language followed by a projected posting in Q1 2020.

Project 2019-02 BES Cyber System Information Access Management (agenda item 6a)
S. Kim provided an overview of Project 2019-02 SAR correction. B. Lawson suggested if a SAR is revised by the SAR drafting team or someone besides the initial SAR requestor, then the SAR requestor field should be updated and a note in revision history be added with the original submitter name.

V. Greaff moved to accept the corrected SAR for Project 2019-02 BES Cyber System Information Access Management.

The Committee approved the motion with no objections or abstentions.

Project 2019-02 BES Cyber System Information Access Management (agenda item 6b)
S. Kim provided an overview of Project 2019-02 posting. B. Lawson motioned to reject the authorization for posting on the basis that it was outside the scope of the approved SAR. He stated that the proposed changes made in CIP-011-3 added low impact assets to the standard's applicability, and that such applicability changes were not explicitly identified in the SAR. L. Harkness and S. Kim explained that the SDT made the revisions to focus attention on the BCSI, and not the classification of the assets, and therefore the changes were within the scope of the Detailed Description portion of the SAR. A. Gallo referenced the Detailed Description section of the SAR which states, "The focus must be on BCSI and the ability to obtain and make use of it." He noted there is no specific mention of high, medium, or low impact assets in the SAR.

B. Lawson moved to reject the authorization for initial posting for Project 2019-02.

The Committee approved the motion with S. Cavote, C. Yeung, R. Shu, and S. Rueckert objecting, and C. Gowder abstaining.

Project 2019-04 Modifications to PRC-005-6 SAR Drafting Team (agenda item 7)
S. Kim provided an overview of the recommended Project 2019-04 SAR Drafting Team. S. Bodkin made a motion to approve the proposed slate with the exclusion of two candidates, citing the SC approved Drafting Team Nominee Selection Criteria that consultants should bring additional technical expertise. S. Kim stated the two candidates proposed to be excluded had drafting team experience and technical expertise, which was why they were recommended by NERC. S. Kim stated if the two candidates were not appointed to the SAR DT, NERC staff would need to solicit for additional nominees for the SAR DT. S. Cavote supported the solicitation for additional nominees, if needed.

S. Bodkin moved to appoint chair, vice chair, and members with the removal of candidates 1 and 7, to Project 2019-04 Modifications to PRC-005-6 Standard Authorization Request (SAR) drafting team.

- Brian Kasmarzik, Ameren Services, chair
- Steve Turner, Arizona Public Service, vice chair
- Giuseppe Giannuzzi, HQCME

- Eric Graftaas, Xcel Energy
- Cesar Huerta, American Electric Power
- Randy Rhinier, Duke Energy
- Sudhir Thakur, Exelon Generation
- Devon Tremont, Taunton Municipal Lighting Plant

The Committee approved the motion with no objections or abstentions.

Technical Committee Update (agenda item 8)
H. Gugel provided an update regarding the restructuring of the NERC Technical Committees, under the Reliability and Security Technical Committee (RSTC). He advised there may be changes to how a SAR is endorsed by the RSTC or one of its subcommittees, and who will participate in the Standards Grading process.

Legal Update (agenda item 9)
L. Perotti provided the legal update regarding recent and upcoming filings.

New Business
J. Flandermeyer suggested a discussion item about consultants on drafting teams be added to the December meeting agenda.

Adjournment
A. Gallo thanked the Committee members and observers and adjourned the meeting at 2:13 p.m. Eastern.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment 1

Segment and Term	Representative	Organization	Proxy	Present (Member or Proxy)
Chair 2018-19	Andrew Gallo Director, Corporate Compliance	City of Austin dba Austin Energy		Yes
Vice Chair 2018-19	Amy Casuscelli Sr. Reliability Standards Analyst	Xcel Energy		Yes
Segment 1-2018-19	Sean Cavote Director NERC Compliance	Public Service Enterprise Group		Yes
Segment 1-2019-20	Sean Bodkin NERC Compliance Policy Manager	Dominion Resources Services, Inc.		Yes
Segment 2-2018-19	Michael Puscas Compliance Manager	ISO New England, Inc.		No
Segment 2-2019-20	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool		Yes
Segment 3-2018-19	Todd Bennett Managing Director, Reliability Compliance & Audit Services	Associated Electric Cooperative, Inc.		Yes
Segment 3-2019-20	Linn Oelker Manager – Market Compliance	LG&E and KU Services Company		Yes
Segment 4-2018-19	Chris Gowder Regulatory Compliance Manager	Florida Municipal Power Agency		Yes
Segment 4-2019-20	Barry Lawson Associate Director, Power Delivery and Reliability	National Rural Electric Cooperative Association		Yes
Segment 5-2018-19	Yee Chou Director NERC Compliance Services	American Electric Power		Yes
Segment 5-2019-20	William Winters Chief Engineer, Electrical Engineering	Con Edison Company of New York, Inc.		Yes

Segment and Term	Representative	Organization	Proxy	Present (Member or Proxy)
Segment 6-2018-19	Jennifer Flandermeyer Director, Federal Regulatory Policy	Evergy Companies		Yes
Segment 6-2019-20	Rebecca Moore Darrah Manager of Reliability Compliance	ACES Power		Yes
Segment 7-2018-19	Frank McElvain Senior Manager, Consulting	Siemens Power Technologies International		No
Segment 7-2019-20	Venona Greaff Senior Energy Analyst	Occidental Chemical Corporation		Yes
Segment 8-2018-19	Robert Blohm Managing Director	Keen Resources Ltd.		No
Segment 8-2019-20	David Kiguel	Independent		Yes
Segment 9-2018-19	Vacant	N/A		N/A
Segment 9-2019-20	Vacant	N/A		N/A
Segment 10-2018-19	Guy Zito Assistant VP of Standards	Northeast Power Coordinating Council	Ruida Shu	Yes
Segment 10-2019-20	Steve Rueckert Director of Standards	WECC		Yes

Standards Committee 2020-2022 Strategic Work Plan

Action

Approve the Standards Committee (SC) 2020-2022 Strategic Work Plan.

Background

A draft SC 2020-2022 Strategic Work Plan was provided for comment to the SC and NERC staff from November 20 to December 2. Based on the comments submitted, a draft plan is attached. Once approved, the plan will be presented to the NERC Board of Trustees for endorsement.

2020-2022 Standards Committee Strategic Work Plan

Introduction

This Standards Committee (SC) Strategic Work Plan (Plan) focuses Standards development activities on: (1) addressing Federal Energy Regulatory Commission (FERC) directives, (2) continuing Periodic Reviews (PRs), and (3) addressing emerging risks using input from various sources, including the Reliability Issues Steering Committee (RISC). The SC will continue: (1) overseeing standards grading activities (evaluating Standards for quality and content), and (2) prioritizing standards development activities.

Emerging Risks

Through input by a NERC technical committee, the RISC or a governmental authority (such as FERC), the SC authorizes the development new or revised Standards, as appropriate.

Vision, Mission and Guiding Principles

Vision

A comprehensive body of Reliability Standards collectively achieving an adequate level of reliability and promoting reliable operation of the North American bulk power system.

Mission

Manage and oversee development of a comprehensive set of Reliability Standards aligned with NERC's strategic goals through open and inclusive processes and procedures.

Guiding Principles

- Consistent with the 2020-2022 Reliability Standards Development Plan (RSDP), this Plan recognizes the transition of the Standard development process to primarily address a small number of FERC directives, Periodic Reviews, and emerging risks. The details of the goals and objectives for 2020-2022 appear in the RSDP.
- Promote and implement a collaborative working environment with other NERC Standing Committees, NERC Standards staff, stakeholders, and standard drafting teams.
- Execute the Standards development process for effective and efficient use of NERC and industry resources.
- Promote and take a leadership role on consensus-building activities.

Work Plan

Task No. 1 – Periodic Reviews

- The Project Management and Oversight Subcommittee (PMOS) and NERC staff prioritize and schedule Periodic Reviews for SC endorsement. PMOS will use the most recent Periodic Review Standing Review Team's grading of Standards to prioritize/schedule by the end of February 2020.

Task No. 2 – Standards Grading

- NERC staff and the SC chair or delegate (acting as facilitator) will start the 2020 Standards grading as soon as practicable to provide time to conduct and comment on the grading. NERC staff will present Standards grading to the SC with the RSDP. To be completed by June 2020 if possible, but no later than the end of August 2020 to coordinate with the development of the 2021-2023 RSDP.

Task No. 3 – Transition of Guidelines and Technical Basis to Technical Rationale

- The SC will continue work to review Guidelines and Technical Basis documents for transition to Technical Rationale documents while moving compliance examples to Implementation Guidance.

Task No. 4 – Standards Committee Process Subcommittee (SCPS)

- NERC staff and the SCPS will endeavor to complete all on-going projects and seek SC endorsement by December 2020. NERC staff and the SCPS will identify opportunities for increased efficiency in existing processes and new processes to enhance Standards development.

Task No. 5 – Fourth Quarter Review of 2020-2022 SC Strategic Work Plan

- The SC will review Plan and provide changes for 2021-2023 to the SC for endorsement.

Task No. 6 – Standards Efficiency Review

- The SC will support the evaluation of NERC Reliability Standards to identify potential efficiencies through retirement or modification of particular requirements. This project seeks to identify potential candidate requirements not necessary for reliability to reduce regulatory obligation.

2019 Standards Committee Accomplishments

Action

Endorse the following Standards Committee Executive Committee (SCEC) determination on the Standards Committee (SC) 2019 accomplishments:

- Periodic Reviews (task 1) – Complete; some projects postponed due to Standards Efficiency Review
- Standards Grading for inclusion in 2019 RSDP (task 2) – N/A; Standards Grading was not conducted in 2019, since Standards Efficiency Review retirements were in process
- Guidelines and Technical Basis transition to Technical Rationale process (task 3) – Complete; remainder of Track 1 Reliability Standards to be posted in early 2020
- Standards Committee Process Subcommittee completion of on-going tasks (task 4) – Complete
- SC conduct a review of its 2018-2020 Strategic Work Plan (task 5) – Complete
- SCEC evaluate the need for additional reforms or enhancements to the SC Charter (task 5) – Complete
- SC support of the Standards Efficiency Review (task 6) – Complete

Background

The 2019-2021 SC Strategic Work Plan required that the SC develop metrics and a self-evaluation process to assess its annual accomplishments. The SCEC reviews each of the annual required tasks and provides the results of whether the SC accomplished each of the required tasks at the December 2019 meeting. Consistent with the review of the SC Strategic Work Plan at the end of 2019, the SCEC uses a binary self-evaluation process to assess the accomplishments and presents the results of each assigned task for the SC's endorsement. The SCEC agreed on the above evaluations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 3a
Standards Committee
December 18, 2019

Three-Month Outlook

Howard Gugel, Vice President of Engineering and Standards, NERC

Standards Committee

December 18, 2019

RELIABILITY | RESILIENCE | SECURITY




Accept / Authorize Standards Authorization Request Postings

- December
  - None
- January
  - None
- February
  - None

Authorize Nomination Solicitations

- December
  - None
- January
  - None
- February
  - None

Authorize Team Appointments

- December
  - Project 2019-06 Cold Weather (SAR DT)
- January
  - None
- February
  - None

Authorize Initial Postings

- December
  - Project 2019-02 BES Cyber System Information Access Management
- January
  - Project 2019-03 Cyber Security Supply Chain Risks
- February
  - None

Standards Efficiency Review (SER)

- Evidence Retention Whitepaper and recommendations Q4 2019
- Data/Information Exchange analysis continues
  - Draft SAR of approximately 13 data/information exchange Requirements with Region/ERO; 6 Requirements become inactive 2022-2027
- CIP SER Working Team – kickoff meeting November 2019
- CIP SER review industry input of recommended retirements

Questions and Answers

Project 2019-02 BES Cyber System Information Access Management

Action

Authorize initial posting for a 45-day formal comment period, with ballot pool formed in the first 30 days and a parallel initial ballot and non-binding poll during the last 10 days of the comment period for the following:

- Proposed Reliability Standards CIP-004-7 and CIP-011-3; and
- The associated Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs).

Background

Project 2019-02 clarified the CIP requirements related to managing access to and securing BES Cyber System Information (BCSI). The standard drafting team (SDT) considered revisions to Reliability Standards CIP-004 and CIP-011 and reviewed the Glossary of Terms Used in NERC Reliability Standards pertaining to requirements addressing BCSI.

This project enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the project seeks to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

This project posting was rejected at the November 20, 2019 Standards Committee meeting. Accordingly, the SDT has made clarifying changes to CIP-011. The SDT revised Requirement R1, Part 1.1 to include the word “applicable” in front of BCSI storage locations to indicate that storage locations of BCSI only related to low impact BES Cyber Systems were not subject to the Reliability Standard.

A Quality Review (QR) on the SDT documents occurred in July 2019. NERC QR staff included Ed Kichline, Soo Jin Kim, Lauren Perotti, and Daniel Bogle. Industry participants were: Alice Ireland (Tri-State Generation and Transmission), Jay Cribb (Southern Company Services, Inc.), Kinte Whitehead (Exelon Corporation), and Kirk Rosener (CPS Energy). The SDT considered all QR inputs and revised the proposed standard where appropriate. J. Hansen (Chair) and Josh Powers (Vice Chair) approved the final documents before submission to the Standards Committee.

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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):
None.

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 by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

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

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

4.1.2.4. 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 Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-004-7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 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 with External Routable Connectivity.

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 BES Cyber Systems Medium Impact BES Cyber Systems	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.	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, emails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 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; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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, 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.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access into a Physical Security Perimeter.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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.

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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access 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 BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) 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 BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and 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 Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	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. (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. (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. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	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. (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. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) 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. (2.2)	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. (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. (2.3)	The Responsible Entity implemented a cyber security 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. (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. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (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. (2.2) OR

R #	Time Horizon	VRF	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 authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			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. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	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. (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 two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	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. (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. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	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. (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 or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 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	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. (3.2 & 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 two individuals. (3.3 & 3.4) OR	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. (3.2 & 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 three individuals. (3.3 & 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 confirm identity for four or more individuals. (3.1 & 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	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. (3.5)	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. (3.5)	or more individuals. (3.2 & 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 four or more individuals. (3.3 & 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	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. (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. (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	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. (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	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic accessor unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	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 BES Cyber Systems, privileges were incorrect or	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 Systems, privileges were incorrect or unnecessary. (4.3)	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 Systems, privileges were incorrect or unnecessary. (4.3)	unescorted physical access have authorization records for at least two consecutive calendar quarters. (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 Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3)			
R5	**Same Day Operations and Operations Planning**	**Medium**	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. (5.3) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (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	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (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	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access 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. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (5.4) 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. (5.2)	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. (5.2)	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. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document 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			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.4)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):
None.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~6~~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 by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~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-~~6~~7:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-004-~~6~~7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 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 with External Routable Connectivity.

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-~~6~~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-~~6~~7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	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.	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

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• 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-~~6~~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-~~6~~7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 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; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, 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-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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, 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.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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 that collectively include each of the applicable requirement parts in *CIP-004-~~6~~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-~~6~~7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed 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-~~6~~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-~~6~~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-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 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.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and~~,~~ unescorted physical access into a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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.

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-~~6~~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-~~6~~7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access 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-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. 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-004-6~~7 Table R5 – Access Revocation			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), 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 associated with the terminations and dated within the next calendar day of the termination action.~~

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 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 BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~5~~4	High Impact BES Cyber Systems and 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 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	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. (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. (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. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	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. (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. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) 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. (2.2)	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. (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. (2.3)	The Responsible Entity implemented a cyber security 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. (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. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (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. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~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 authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			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. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	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. (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 two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	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. (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. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	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. (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 or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 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	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. (3.2 & 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 two individuals. (3.3 & 3.4) OR	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. (3.2 & 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 three individuals. (3.3 & 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 confirm identity for four or more individuals. (3.1 & 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	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. (3.5)	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. (3.5)	or more individuals. (3.2 & 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 four or more individuals. (3.3 & 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	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. (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. (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	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. (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	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access~~,~~or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~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 BES Cyber Systems, privileges were incorrect or	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 Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information 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 BES Cyber System Information storage locations, privileges were~~	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 Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information 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 storage locations, privileges were~~	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. (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 Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage~~	~~incorrect or unnecessary. (4.4)~~	~~incorrect or unnecessary. (4.4)~~	incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~locations, privileges were incorrect or unnecessary. (4.4)~~			
R5	**Same Day Operations and Operations Planning**	**Medium**	~~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 Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or~~,~~ unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of the termination action. (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. (5.4~~3~~) OR The Responsible	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. (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 Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the~~	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. (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 Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective~~	removals for three or more individuals. (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. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (5.~~5~~4) OR The Responsible	~~termination action. (5.3)~~	~~date and time of the termination action. (5.3)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document 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. (5.~~5~~4)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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 security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.~~

~~Examples of possible mechanisms and evidence, when dated, which can be used are:~~

~~Direct communications (e.g., emails, memos, computer based training, etc.);~~

~~Indirect communications (e.g., posters, intranet, brochures, etc.);~~

~~Management support and reinforcement (e.g., presentations, meetings, etc.).~~

~~Requirement R2:~~

~~Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.~~

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

~~Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.~~

~~Requirement R3:~~

~~Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.~~

~~A seven-year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing~~

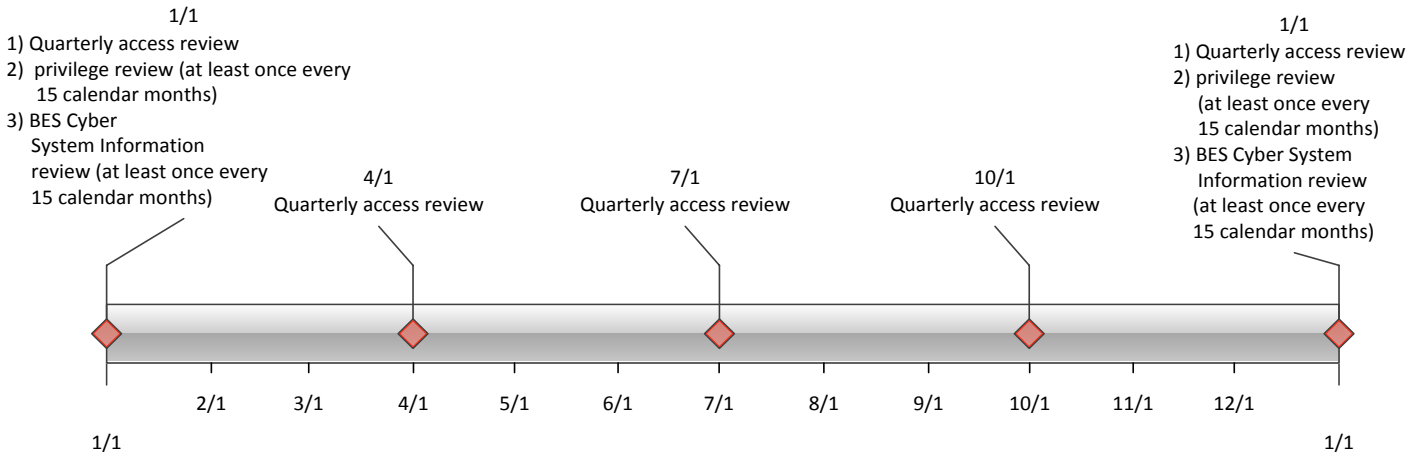
~~collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.~~

~~Requirement R4:~~

~~Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.~~

~~This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.~~

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

~~Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.~~

~~If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.~~

~~For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.~~

~~Requirement R5:~~

~~The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.~~

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

~~Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.~~

~~Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.~~

~~**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:**~~

~~Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.~~

~~**Rationale for Requirement R2:**~~

~~To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.~~

~~**Rationale for Requirement R3:**~~

~~To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.~~

~~**Rationale for Requirement R4:**~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

~~Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).~~

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

~~Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.~~

~~If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.~~

~~For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.~~

~~Rationale for Requirement R5:~~

~~The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.~~

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.~~

~~Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).~~

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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):
None.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information 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 or 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 Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-011-3.

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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicability Systems" column further defines 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 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 Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	System information pertaining to: 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	Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Storage locations identified for housing BES Cyber System Information in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information and key management program, retention in the Physical Security Perimeter).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key management program. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	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 from the BES Cyber Asset. (3.1)	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 from the BES Cyber Asset. (3.1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R3)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):
None.

A. Introduction

1. Title: Cyber Security — Information Protection

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

3. Purpose: To prevent unauthorized access to BES Cyber System Information 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-~~2~~3:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-011-~~2~~3.

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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicability Systems" column ~~to~~ further defines 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-~~2~~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-~~2~~3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.1	System information pertaining to: High ~~-~~Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA	~~Method~~Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented ~~method~~ process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • ~~Repository or electronic and physical~~ Storage locations identified ~~designated~~ for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~PACS~~	~~Procedure~~Method(s) to prevent unauthorized access to ~~for protecting and securely handling~~ BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during~~, including~~ storage, transit, use, and disposal~~-~~.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to ~~Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of~~ BES Cyber System Information (e.g., encryption of ~~; or~~ • ~~Records indicating that~~ BES Cyber System Information and key management program, retention in the Physical Security Perimeter)~~is handled in a manner consistent with the entity's documented procedure(s)~~.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3~~2~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M~~2~~3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~3~~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	Prior to the release for reuse or disposal 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 from~~ the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • ~~Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information 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.~~ Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

~~CIP-011-2 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 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)~~N/A~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**~~Lower~~Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						management program. (R2)
R~~2~~3	**Operations Planning**	**Lower**	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 from the BES Cyber Asset. (~~2~~3.1)	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 from the BES Cyber Asset. (~~2~~3.~~2~~1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal. (R~~2~~3)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~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	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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.

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3.

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Establish and/or modify vendor relationships to establish compliance with the revised CIP-011-3 Requirements;
- Address the increased scope of the CIP-011-3 "Applicable Systems" and "Applicability" column, which has a focus on BES Cyber System Information as well as the addition of Protected Cyber Assets (PCA); and
- Develop additional sanitization programs for the life cycle of BES Cyber Systems, if necessary.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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

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

CIP-011-3 – Cyber Security - Information Protection

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

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

Retirement Date

CIP-004-7 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-3 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-011-3, Requirement R1

Requirement R1 was revised to include PCA and eliminate potential barriers to use cloud based services for storage of BES Cyber System Information. No changes to the VRF are necessary from the previously approved standard. The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning time horizon to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	**Guideline 2- Consistency within a Reliability Standard** The requirement has sub-requirements and is assigned a single VRF consistent with other Requirements within the proposed standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective, which is to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-011-3, R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during	The Responsible Entity has not documented or implemented any processes for BES Cyber System Information protection (R2)

		storage, transit, use and disposal (Part 1.2)	

VSL Justifications for CIP-001-3, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-001-3, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection.

VRF Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4(CIP-011-3 Requirement R1, Part 1.6) and a portion of Part 4.1(CIP-011-3 Requirement R1, Part 1.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5

The VSL has been revised to reflect the removal of Part 5.3(CIP-011-3 Requirement R1, Part 1). The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

Project 2019-05 Modifications to PER-003-2

Action

- Accept the revised Project 2019-05 Modifications to PER-003-2 Standard Authorization Request (SAR);
- Authorize drafting revisions to the Reliability Standards identified in the SAR; and
- Appoint the Project 2019-05 Modifications to PER-003-2 SAR Drafting Team (DT) as the Project 2019-05 Standard Drafting Team (SDT).

Background

On July 9, 2019, the Chair of the Personnel Certification Governance Committee (PCGC) submitted a SAR to revise PER-003-2 so that one credential would be required, instead of the four credentials referenced in the current standard. The SAR followed the development of a PCGC whitepaper titled *One System Operator Certification Credential*. In this whitepaper, the PCGC proposed that the current System Operator Certification be changed from its current four credentials to one credential.

On July 24, 2019, the Standards Committee accepted the SAR, authorized posting for a 30-day informal comment period, and authorized for solicitation of SAR drafting team members. The Standards Committee appointed the SAR drafting team on October 23, 2019.

The SAR DT met November 8, 2019 to review and make revisions to the SAR. The team considered industry comments during this process. Consideration of Comments can be found on the Project 2019-05 page.

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:	Modification to PER-003-2		
Date Submitted:	09 July 2019		
SAR Requester			
Name:	Personnel Certification and Governance Committee (Chair – Mike Anderson)		
Organization:	NERC		
Telephone:	(614) 413-2311	Email:	mcanderson@aep.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?):			
Enhanced BES Reliability			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Referencing the PCGC's "One System Operator Certification credential" whitepaper, all System Operators would hold the same Certification credential. This better serves reliability by ensuring all System Operators, regardless of their company's registration or credential of choice, have the same base knowledge. This knowledge is demonstrated through the System Operator Certification process.			
Project Scope (Define the parameters of the proposed project):			
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. Team will develop the implementation plan timeline in coordination with the PCGC transition plan. ~~Modification of PER-003-2 through the Standards Development Process~~			

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):
Modify Reliability Standard PER-003-2 by consolidating four separate System Operation Certification credentials into a single credential. ~~Revise PER-003-2 to address one credential is required, not the current four credentials.~~ PER-005 did not exist at the inception of system operator certification. PER-003-2 is a personal certification of minimal knowledge and skills; whereas PER-005 addresses more specific reliability related tasks for entity qualifications/requirements. The team will consider the relationship between PER-003-2 and PER-005-2 as well as the relationship between PER-003-2 and the System Operator Certification Program Manual. ~~To address any potential gaps concerning the misconception of applicable areas of competency, please consider making a stronger tie between the revised PER-003-2 to PER-005. It is still important to maintain the independence of each Standard.~~
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Minimal cost impact to industry as bundled in the PCGC's budget recovered through existing exam and renewal fees.
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):
Reliability Coordinator, Transmission Operator, Balancing Authority
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.
Industry circulated "One Credential" whitepaper and associated comments/responses from the PCGC
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)?
None
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐ DRAFT SAR approved for posting by the SC	☐ 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

Project 2019-06 Cold Weather SAR Drafting Team

Action

Appoint chair, vice chair, and members to the Project 2019-06 Cold Weather Standard Authorization Request (SAR) drafting team, as recommended by NERC staff.

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 bulk electric system during cold weather events by ensuring that entities prepare for extreme cold weather conditions.

The Standards Committee accepted the SAR and authorized soliciting for members for the SAR DT on October 2, 2019. From October 4 to November 5, 2019, NERC solicited nominations for a SAR drafting team. NERC staff received twenty (20) nominations and recommends twelve (12) individuals with the requisite background, experience, and skills necessary for membership on the SAR drafting team.

Project 2015-09 Establish and Communicate System Operating Limits

Action

Appoint chair to the standard drafting team (SDT) for Project 2015-09, as recommended by NERC staff.

Background

Due to personnel and other changes, the current chair of the Project 2015-09 SDT had to transition out of the role. NERC staff recommends that the Standards Committee appoint Dean LaForest (ISO New England), a current member of the SDT, as chair.

The purpose of Project 2015-09 is to revise the requirements for determining and communicating System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs) to address the issues identified in Project 2015-03 Periodic Review of System Operating Limit Standards. The resulting standard(s) and definition(s) will benefit reliability by improving alignment with approved Transmission Planning (TPL) and proposed Transmission Operations (TOP) and Interconnection Reliability Operations and Coordination (IRO) standards. The project may result in development of one or more proposed Reliability Standards and definitions.

Project 2017-01 Modifications to BAL-003-1.1

Action

Approve errata to Reliability Standard BAL-003-2.

Background

The NERC Standard Processes Manual Section 12.0: Process for Correcting Errata states:

> "From time to time, an error may be discovered in a Reliability Standard. Such errors may be corrected (i) following a Final Ballot prior to Board of Trustees adoption, (ii) following Board of Trustees adoption prior to filing with Applicable Governmental Authorities; and (iii) following filing with Applicable Governmental Authorities. If the Standards Committee agrees that the correction of the error does not change the scope or intent of the associated Reliability Standard, and agrees that the correction has no material impact on the end users of the Reliability Standard, then the correction shall be filed for approval with Applicable Governmental Authorities as appropriate. The NERC Board of Trustees has resolved to concurrently approve any errata approved by the Standards Committee."

Summary

The purpose of proposed Reliability Standard BAL-003-2 is to "To require sufficient Frequency Response from the Balancing Authority (BA) to maintain Interconnection Frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value. To provide consistent methods for measuring Frequency Response and determining the Frequency Bias Setting." The proposed standard achieved a 100% approval with 92.96% quorum, and was adopted by the NERC Board of Trustees on November 5, 2019.

Under the standard, each year, the ERO, in consultation with regional representatives, establishes an Interconnection Frequency Obligation (IFRO) for each of the four North American Interconnections. This IFRO is then used to establish the obligations of Balancing Authorities in that Interconnection to provide frequency response. The IFRO is established in accordance with Attachment A to the standard, calculated in accordance with a set mathematical formula with the processes set forth in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard.*

In proposed Reliability Standard BAL-003-2, the drafting team revised Attachment A and the *Procedure*, including the mathematical formula used to determine IFRO. As an illustration, the team provided in Table A the resulting target values from this calculation. These values are appropriately labeled target values, and as noted in the standard, they remain subject to annual review and revision. In the case of the Eastern Interconnection, these targets were lowered in

increments over three years with additional provisions for analysis to prevent undesirable reliability impacts.

Before finalizing these target values for the final ballot, the drafting team voted to adjust the final step target IFRO value for the Eastern Interconnection from the number produced by the mathematical formula (-764 MW/.1Hz) to reflect the lowest IFRO value that had been successfully validated by NERC staff's studies. This final step target IFRO value was incorrectly captured in Table A (and repeated in the *Procedure*) as -784 MW/.1Hz, while the correct value is -787 MW/.1Hz. In addition, due to the *Procedure* being revised*, t*he hyperlink to the previous version of the *Procedure* was removed in the Attachment.

Correction of the errors will not change the scope or intent of the associated Reliability Standard. Correction of the errors will not change the process nor the mathematical formula to be used for IFRO calculations. As noted above, the official IFROs are determined and validated annually by NERC in accordance with Attachment A and the *Procedure* and it is those official IFRO values, not the target values in Table A, that establish the obligations of the Balancing Authorities per the requirements. For these same reasons, correction of the errors will have no material impact on the end users of the Reliability Standard.

The changes are illustrated below:

Attachment A

BAL-003-2 Frequency Response and Frequency Bias Setting Standard

Supporting Document

Interconnection Frequency Response Obligation

The ERO, in consultation with regional representatives, has established a target reliability criterion for each Interconnection called the Interconnection Frequency Response Obligation (IFRO). Preliminary values are provided below. Certain values are assessed annually according to the methodology which is detailed in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard.*

Chris Larson
Formatted: Font: Italic

Interconnection	Eastern	Western	ERCOT	HQ	Units
Max. Delta Frequency (MDF)	0.420	0.280	0.405	0.947	
Resource Loss Protection Criteria (RLPC)[1]	3,209	2,850	2,750	2,000	MW
Credit for Load Resources (CLR)			1,209		MW
Current IFRO (OY 2018)	-1,015	-858	-381	-179	MW/0.1 Hz
First-Step target IFRO[1]	-915	-1018	-380	-211	MW/0.1 Hz
Second-Step target IFRO[1, 2]	-815				
Final target IFRO[1, 2]	~~-784~~ 787				

Table 1: Interconnection Frequency Response Obligations (base year 2017)

IFRO = (RLPC – CLR)/Max Delta Freq/10

1. *These values are evaluated annually for changes in each Interconnection.*
2. *To reduce risk, the Eastern Interconnection IFRO will be stepped down annually from the 2017 value of -1,015 MW/0.1 Hz in -100 MW/0.1 Hz increments. If during the step down process, Interconnection Frequency Response Measure (FRM) declines by more than 10 percent, the ERO will halt the reduction in IFRO until such time that a determination can be made as to the cause of the degradation.*

A. Introduction

1. **Title: Frequency Response and Frequency Bias Setting**

2. **Number: BAL-003-2**

3. **Purpose:** To require sufficient Frequency Response from the Balancing Authority (BA) to maintain Interconnection Frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value. To provide consistent methods for measuring Frequency Response and determining the Frequency Bias Setting.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

   4.1.1.1. Balancing Authority is the responsible entity unless the Balancing Authority is a member of a Frequency Response Sharing Group, in which case, the Frequency Response Sharing Group becomes the responsible entity.

   4.1.2. Frequency Response Sharing Group

5. **Effective Date:** See Implementation Plan for BAL-003-2.

B. Requirements and Measures

R1. Each Frequency Response Sharing Group (FRSG) or Balancing Authority that is not a member of a FRSG shall achieve an annual Frequency Response Measure (FRM) (as calculated and reported in accordance with Attachment A) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each FRSG or BA that is not a member of a FRSG to maintain Interconnection Frequency Response equal to or more negative than the Interconnection Frequency Response Obligation. *[Risk Factor: High][Time Horizon: Real-time Operations]*

M1. Each Frequency Response Sharing Group or Balancing Authority that is not a member of a Frequency Response Sharing Group shall have evidence such as dated data plus documented formula in either hardcopy or electronic format that it achieved an annual FRM (in accordance with the methods specified by the ERO in Attachment A with data from FRS Form 1 reported to the ERO as specified in Attachment A) that is equal to or more negative than its FRO to demonstrate compliance with Requirement R1.

R2. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting shall implement the Frequency Bias Setting determined in

accordance with Attachment A, as validated by the ERO, into its Area Control Error (ACE) calculation during the implementation period specified by the ERO and shall use this Frequency Bias Setting until directed to change by the ERO. *[Risk Factor: Medium][Time Horizon: Operations Planning]*

M2. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service shall have evidence such as a dated document in hard copy or electronic format showing the ERO validated Frequency Bias Setting was implemented into its ACE calculation within the implementation period specified or other evidence to demonstrate compliance with Requirement R2.

R3. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and is utilizing a variable Frequency Bias Setting shall maintain a Frequency Bias Setting that is: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

3.1 Less than zero at all times, and

3.2 Equal to or more negative than its Frequency Response Obligation when Frequency varies from 60 Hz by more than +/- 0.036 Hz.

M3. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection, is not receiving Overlap Regulation Service and is utilizing variable Frequency Bias shall have evidence such as a dated report in hard copy or electronic format showing the average clock-minute average Frequency Bias Setting was less than zero and during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was equal to or more negative than its Frequency Response Obligation to demonstrate compliance with Requirement R3.

R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify its Frequency Bias Setting in its ACE calculation, in order to represent the Frequency Bias Setting for the combined Balancing Authority Area, to be equivalent to either: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

- The sum of the Frequency Bias Settings as shown on FRS Form 1 and FRS Form 2 for the participating Balancing Authorities as validated by the ERO, or

- The Frequency Bias Setting shown on FRS Form 1 and FRS Form 2 for the entirety of the participating Balancing Authorities' Areas.

M4. The Balancing Authority shall have evidence such as a dated operating log, database or list in hard copy or electronic format showing that when it performed Overlap Regulation Service, it modified its Frequency Bias Setting in its ACE calculation as specified in Requirement R4 to demonstrate compliance with Requirement R4.

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 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 Balancing Authority shall retain data or evidence to show compliance with Requirements R1, R2, R3 and R4, Measures M1, M2, M3 and M4 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- The Frequency Response Sharing Group shall retain data or evidence to show compliance with Requirement R1 and Measure M1 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- If a Balancing Authority or Frequency Response Sharing Group is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all subsequent requested and submitted 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.

- For Interconnections that are also Balancing Authorities, Tie Line Bias control and flat frequency control are equivalent and either is acceptable.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by at most 15% or 15 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 15% but by at most 30% or 30 MW/0.1 Hz, whichever is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 30% but by at most 45% or 45 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 45% or by more than 45 MW/0.1 Hz, whichever is the greater deviation from its FRO.
R2.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting failed to implement the validated Frequency Bias Setting value into its ACE calculation within the implementation period specified but did so within 5 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 5 calendar days but less than or equal to 15 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 15 calendar days but less than or equal to 25 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting did not implement the validated Frequency Bias Setting value into its ACE calculation in more than 25 calendar days from the implementation period specified by the ERO.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 1% but by at most 10%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 10% but by at most 20%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 20% but by at most 30%.	The Balancing Authority that is a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response obligation by more than 30%.
R4.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error less than or equal to 10% of the validated or calculated value.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 10% but less than or equal to 20% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 20% but less than or equal to 30% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 30% of the validated or calculated value. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		validated or calculated value.	validated or calculated value.	The Balancing Authority failed to change the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services.

D. Regional Variances

None.

E. Associated Documents

Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

FRS Form 1

FRS Form 2

Frequency Response Standard Background Document

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	March 16, 2007	FERC Approval — Order 693	New
0a	December 19, 2007	Added Appendix 1 — Interpretation of R3 approved by BOT on October 23, 2007	Addition
0a	July 21, 2008	FERC Approval of Interpretation of R3	Addition
0b	February 12, 2008	Added Appendix 2 — Interpretation of R2, R2.2, R5, and R5.1 approved by BOT on February 12, 2008	Addition
0.1b	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial; updated version number to “0.1b”	Errata
0.1b	October 29, 2008	BOT approved errata changes	Errata
0.1a	May 13, 2009	FERC Approved errata changes – version changed to 0.1a (Interpretation of R2, R2.2, R5, and R5.1 not yet approved)	Errata
0.1b	May 21, 2009	FERC Approved Interpretation of R2, R2.2, R5, and R5.1	Addition
1	February 7, 2013	Adopted by NERC Board of Trustees	Complete Revision under Project 2007-12
1	January 16, 2014	FERC Order issued approving BAL-003-1. (Order becomes effective for R2, R3, and R4 April 1, 2015. R1 becomes effective April 1, 2016.)	
1	May 7, 2014	NERC Board of Trustees adopted revisions to VRF and VSLs in Requirement R1.	
1	November 26, 2014	FERC issued a letter order approved VRF and VSL revisions to Requirement R1.	

Version	Date	Action	Change Tracking
1.1	August 25, 2015	Added numbering to Introduction section, corrected parts numbering for R3, and adjusted font within section M4.	Errata
1.1	November 13, 2015	FERC Letter Order approved errata to BAL-003-1.1. Docket RD15-6-000	Errata
2	November 5, 2019	NERC Board of Trustees adopted BAL-003-2	New

Attachment A

BAL-003-2 Frequency Response and Frequency Bias Setting Standard

Supporting Document

Interconnection Frequency Response Obligation

The ERO, in consultation with regional representatives, has established a target reliability criterion for each Interconnection called the Interconnection Frequency Response Obligation (IFRO). Preliminary values are provided below. Certain values are assessed annually according to the methodology which is detailed in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*.

Interconnection	**Eastern**	**Western**	**ERCOT**	**HQ**	Units
Max. Delta Frequency (MDF)	**0.420**	**0.280**	**0.405**	**0.947**	
Resource Loss Protection Criteria (RLPC)[1]	**3,209**	**2,850**	**2,750**	**2,000**	MW
Credit for Load Resources (CLR)			**1,209**		MW
Current IFRO (OY 2018)	**-1,015**	**-858**	**-381**	**-179**	MW/0.1 Hz
First-Step target IFRO[1]	**-915**	**-1018**	**-380**	**-211**	MW/0.1 Hz
Second-Step target IFRO[1, 2]	**-815**				
Final target IFRO[1, 2]	**-787**				

Table 1: Interconnection Frequency Response Obligations (base year 2017)

IFRO = (RLPC – CLR)/Max Delta Freq/10

1. *These values are evaluated annually for changes in each Interconnection.*
2. *To reduce risk, the Eastern Interconnection IFRO will be stepped down annually from the 2017 value of -1,015 MW/0.1 Hz in -100 MW/0.1 Hz increments. If during the step down process, Interconnection Frequency Response Measure (FRM) declines by more than 10 percent, the ERO will halt the reduction in IFRO until such time that a determination can be made as to the cause of the degradation.*

Balancing Authority Frequency Response Obligation and Frequency Bias Setting

For a multiple Balancing Authority interconnection, the Interconnection FRO shown in Table 1 is allocated based on the Balancing Authority annual load and annual generation. The FRO allocation will be based on the following method:

$$\text{FRO}_{\text{BA}} = \text{IFRO} \quad \times \frac{\text{Annual Gen}_{\text{BA}} + \text{Annual Load}_{\text{BA}}}{\text{Annual Gen}_{\text{Int}} + \text{Annual Load}_{\text{Int}}}$$

Where:

- Annual Gen_{BA} is the total annual output of generating plants within the Balancing Authority Area (BAA).
- Annual Load_{BA} is total annual Load within the BAA.
- Annual Gen_{Int} is the sum of all Annual Gen_{BA} values reported in that interconnection.
- Annual Load_{Int} is the sum of all Annual Load_{BA} values reported in that interconnection.

Balancing Authorities that elect to form a FRSG will calculate a FRSG FRO by adding together the individual BA FRO's.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_{A} and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Submit a joint Form 1 with the "FRSG" tab completed for the aggregate performance of the participating Balancing Authorities.

Balancing Authorities that merge or transfer load or generation are encouraged to notify the ERO of the change in footprint and corresponding changes in allocation such that the net obligation to the Interconnection remains the same and so that CPS limits can be adjusted.

Each Balancing Authority reports its previous year's FRM, Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO each year to allow the ERO to validate the revised Frequency Bias Settings on FRS Form 1. In addition, each Balancing Authority will report its two largest potential resource losses and any applicable N-2 RAS events in the form. If the ERO posts the official list of events after the date specified in the timeline below, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1.

Once the ERO reviews the data submitted in FRS Form 1 and FRS Form 2 for all Balancing Authorities, the ERO will use FRS Form 1 data to post the following information for each Balancing Authority for the upcoming year:

- Frequency Bias Setting
- Frequency Response Obligation (FRO)

Once the data listed above is fully posted, the ERO will announce the three-day implementation period for changing the Frequency Bias Setting if it differs from that shown in the timeline below.

A Balancing Authority using a fixed Frequency Bias Setting sets its Frequency Bias Setting to the greater of (in absolute value):

- Any number the Balancing Authority chooses between 100 percent and 125 percent of its Frequency Response Measure as calculated on FRS Form 1
- Interconnection Minimum as determined by the ERO

For purposes of calculating the minimum Frequency Bias Setting, a Balancing Authority participating in a FRSG will need to calculate its stand-alone FRM using FRS Form 1 and FRS Form 2 to determine its minimum Frequency Bias Setting.

A Balancing Authority providing Overlap Regulation will report the historic peak demand and generation of its combined Balancing Authorities' areas on FRS Form 1 as described in Requirement R4.

Frequency Response Measure

The Balancing Authority will calculate its FRM from Single Event Frequency Response Data (SEFRD), defined as: "the data from an individual event in a Balancing Authority area that is used to calculate its Frequency Response, expressed in MW/0.1Hz" as calculated on FRS Form 2 for each event shown on FRS Form 1. The events in FRS Form 1 are selected by the ERO using the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*. The SEFRD for a typical Balancing Authority in an Interconnection with more than one Balancing Authority is the change in its Net Actual Interchange on its tie lines with adjacent Balancing Authorities divided by the change in Interconnection frequency. Some Balancing Authorities may choose to apply corrections to their Net Actual Interchange (NA_I) values to account for factors such as nonconforming loads. FRS Form 1 and 2 shows the types of adjustments that are allowed. Note that with the exception of the Contingent BA column, any adjustments made must be made for all events in an evaluation year.[1]

The ERO will use a standardized sampling interval of approximately 16 seconds before the event, up to the time of the event for the pre-event NA_I, and frequency (A values), and approximately 20 to 52 seconds after the event for the post-event NA_I (B values) in the computation of SEFRD values, dependent on the data scan rate of the Balancing Authority's Energy Management System (EMS).

All events listed on FRS Form 1 need to be included in the annual submission of FRS Forms 1 and 2. The only time a Balancing Authority should exclude an event is if its tie-line data or its Frequency data is corrupt, or its EMS was unavailable. FRS Form 2 has instructions on how to

[1] As an example, if an entity has non-conforming loads and makes an adjustment for one event, all events must show the non-conforming load, even if the non-conforming load does not impact the calculation. This ensures that the reports are not utilizing the adjustments only when they are favorable to the BA.

correct the BA's data if the given event is internal to the BA or if other authorized adjustments are used.

Assuming data entry is correct, FRS Form 1 will automatically calculate the Balancing Authority's FRM for the past 12 months as the median of the SEFRD values. A Balancing Authority electing to report as an FRSG or a provider of Overlap Regulation Service will provide an FRS Form 1 for the aggregate of its participants.

To allow Balancing Authorities to plan its operations, events with a "Point C" that cause the Interconnection Frequency to be lower than that shown in Table 1 above (for example, an event in the Eastern Interconnection that causes the Interconnection Frequency to go to 59.4 Hz) or higher than an equal change in frequency going above 60 Hz may be included in the list of events for that Interconnection. However, the calculation of the Balancing Authority response to such an event will be adjusted to show a frequency change only to the Target Minimum Frequency shown in Table 1 above (in the previous example this adjustment would cause Frequency to be shown as 59.5 Hz rather than 59.4 HZ) or a high frequency amount of an equal quantity. Should such an event happen, the ERO will provide additional guidance.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_A and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Jointly submit the individual Balancing Authority's Form 1s, with a summary spreadsheet that contains the sum of each participant's individual event performance.

Timeline for Balancing Authority Frequency Response and Frequency Bias Setting Activities

Described below is the timeline for the exchange of information between the ERO and Balancing Authorities to:

- Facilitate the assignment of Balancing Authority FRO
- Calculate Balancing Authority FRM
- Determine Balancing Authority Frequency Bias Settings

Target Business Date	Activity
March 1	**FRS Form 1 is posted by the ERO* with all selected events for the operating year for BA usage.**
April 1	**BAs and FRSGs complete their frequency response forms for all four quarters, including the BAs' FBS calculations, returning the results to the ERO.**
May 1	**The ERO validates FBS values, computes the sum of all FBS values for each Interconnection.**
May 15	**The BAs not required to file FERC Form 714 receive a request to provide load and generation data as described in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*** **to support FRO assignments and determining minimum FBS for the upcoming year. Data to be provided by July 15.**
June 1	The BA implements any changes to their FBS.
November 1	The ERO assigns FRO values and Minimum FBS for the upcoming year to the BAs.

* If 4th quarter posting of FRS Form 1s is delayed, the ERO may adjust the other timelines in this table by a similar amount.

** Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

A. Introduction

1. **Title: Frequency Response and Frequency Bias Setting**

2. **Number: BAL-003-2**

3. **Purpose:** To require sufficient Frequency Response from the Balancing Authority (BA) to maintain Interconnection Frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value. To provide consistent methods for measuring Frequency Response and determining the Frequency Bias Setting.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Balancing Authority

   4.1.1.1. Balancing Authority is the responsible entity unless the Balancing Authority is a member of a Frequency Response Sharing Group, in which case, the Frequency Response Sharing Group becomes the responsible entity.

   4.1.2. Frequency Response Sharing Group

5. **Effective Date:** See Implementation Plan for BAL-003-2.

B. Requirements and Measures

R1. Each Frequency Response Sharing Group (FRSG) or Balancing Authority that is not a member of a FRSG shall achieve an annual Frequency Response Measure (FRM) (as calculated and reported in accordance with Attachment A) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each FRSG or BA that is not a member of a FRSG to maintain Interconnection Frequency Response equal to or more negative than the Interconnection Frequency Response Obligation. *[Risk Factor: High][Time Horizon: Real-time Operations]*

M1. Each Frequency Response Sharing Group or Balancing Authority that is not a member of a Frequency Response Sharing Group shall have evidence such as dated data plus documented formula in either hardcopy or electronic format that it achieved an annual FRM (in accordance with the methods specified by the ERO in Attachment A with data from FRS Form 1 reported to the ERO as specified in Attachment A) that is equal to or more negative than its FRO to demonstrate compliance with Requirement R1.

R2. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting shall implement the Frequency Bias Setting determined in

accordance with Attachment A, as validated by the ERO, into its Area Control Error (ACE) calculation during the implementation period specified by the ERO and shall use this Frequency Bias Setting until directed to change by the ERO. *[Risk Factor: Medium][Time Horizon: Operations Planning]*

M2. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service shall have evidence such as a dated document in hard copy or electronic format showing the ERO validated Frequency Bias Setting was implemented into its ACE calculation within the implementation period specified or other evidence to demonstrate compliance with Requirement R2.

R3. Each Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and is utilizing a variable Frequency Bias Setting shall maintain a Frequency Bias Setting that is: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

3.1 Less than zero at all times, and

3.2 Equal to or more negative than its Frequency Response Obligation when Frequency varies from 60 Hz by more than +/- 0.036 Hz.

M3. The Balancing Authority that is a member of a multiple Balancing Authority Interconnection, is not receiving Overlap Regulation Service and is utilizing variable Frequency Bias shall have evidence such as a dated report in hard copy or electronic format showing the average clock-minute average Frequency Bias Setting was less than zero and during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was equal to or more negative than its Frequency Response Obligation to demonstrate compliance with Requirement R3.

R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify its Frequency Bias Setting in its ACE calculation, in order to represent the Frequency Bias Setting for the combined Balancing Authority Area, to be equivalent to either: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

- The sum of the Frequency Bias Settings as shown on FRS Form 1 and FRS Form 2 for the participating Balancing Authorities as validated by the ERO, or

- The Frequency Bias Setting shown on FRS Form 1 and FRS Form 2 for the entirety of the participating Balancing Authorities' Areas.

M4. The Balancing Authority shall have evidence such as a dated operating log, database or list in hard copy or electronic format showing that when it performed Overlap Regulation Service, it modified its Frequency Bias Setting in its ACE calculation as specified in Requirement R4 to demonstrate compliance with Requirement R4.

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 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 Balancing Authority shall retain data or evidence to show compliance with Requirements R1, R2, R3 and R4, Measures M1, M2, M3 and M4 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- The Frequency Response Sharing Group shall retain data or evidence to show compliance with Requirement R1 and Measure M1 for the current year plus the previous three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- If a Balancing Authority or Frequency Response Sharing Group is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all subsequent requested and submitted 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.

- For Interconnections that are also Balancing Authorities, Tie Line Bias control and flat frequency control are equivalent and either is acceptable.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by at most 15% or 15 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 15% but by at most 30% or 30 MW/0.1 Hz, whichever is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 30% but by at most 45% or 45 MW/0.1 Hz, whichever one is the greater deviation from its FRO.	The Balancing Authority's, or Frequency Response Sharing Group's, FRM was less negative than its FRO by more than 45% or by more than 45 MW/0.1 Hz, whichever is the greater deviation from its FRO.
R2.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting failed to implement the validated Frequency Bias Setting value into its ACE calculation within the implementation period specified but did so within 5 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 5 calendar days but less than or equal to 15 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting implemented the validated Frequency Bias Setting value into its ACE calculation in more than 15 calendar days but less than or equal to 25 calendar days from the implementation period specified by the ERO.	The Balancing Authority in a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a fixed Frequency Bias Setting did not implement the validated Frequency Bias Setting value into its ACE calculation in more than 25 calendar days from the implementation period specified by the ERO.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and is not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 1% but by at most 10%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 10% but by at most 20%.	The Balancing Authority that is a member of a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response Obligation by more than 20% but by at most 30%.	The Balancing Authority that is a multiple Balancing Authority Interconnection and not receiving Overlap Regulation Service and uses a variable Frequency Bias Setting average Frequency Bias Setting during periods when the clock-minute average frequency was outside of the range 59.964 Hz to 60.036 Hz was less negative than its Frequency Response obligation by more than 30%.
R4.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error less than or equal to 10% of the validated or calculated value.	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 10% but less than or equal to 20% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 20% but less than or equal to 30% of the	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint setting-error more than 30% of the validated or calculated value. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		validated or calculated value.	validated or calculated value.	The Balancing Authority failed to change the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services.

D. Regional Variances

None.

E. Associated Documents

Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

FRS Form 1

FRS Form 2

Frequency Response Standard Background Document

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	March 16, 2007	FERC Approval — Order 693	New
0a	December 19, 2007	Added Appendix 1 — Interpretation of R3 approved by BOT on October 23, 2007	Addition
0a	July 21, 2008	FERC Approval of Interpretation of R3	Addition
0b	February 12, 2008	Added Appendix 2 — Interpretation of R2, R2.2, R5, and R5.1 approved by BOT on February 12, 2008	Addition
0.1b	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial; updated version number to “0.1b”	Errata
0.1b	October 29, 2008	BOT approved errata changes	Errata
0.1a	May 13, 2009	FERC Approved errata changes – version changed to 0.1a (Interpretation of R2, R2.2, R5, and R5.1 not yet approved)	Errata
0.1b	May 21, 2009	FERC Approved Interpretation of R2, R2.2, R5, and R5.1	Addition
1	February 7, 2013	Adopted by NERC Board of Trustees	Complete Revision under Project 2007-12
1	January 16, 2014	FERC Order issued approving BAL-003-1. (Order becomes effective for R2, R3, and R4 April 1, 2015. R1 becomes effective April 1, 2016.)	
1	May 7, 2014	NERC Board of Trustees adopted revisions to VRF and VSLs in Requirement R1.	
1	November 26, 2014	FERC issued a letter order approved VRF and VSL revisions to Requirement R1.	

Version	Date	Action	Change Tracking
1.1	August 25, 2015	Added numbering to Introduction section, corrected parts numbering for R3, and adjusted font within section M4.	Errata
1.1	November 13, 2015	FERC Letter Order approved errata to BAL-003-1.1. Docket RD15-6-000	Errata
2	November 5, 2019	NERC Board of Trustees adopted BAL-003-2	New

Attachment A

BAL-003-2 Frequency Response and Frequency Bias Setting Standard

Supporting Document

Interconnection Frequency Response Obligation

The ERO, in consultation with regional representatives, has established a target reliability criterion for each Interconnection called the Interconnection Frequency Response Obligation (IFRO). Preliminary values are provided below. Certain values are assessed annually according to the methodology which is detailed in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard.*

Interconnection	**Eastern**	**Western**	**ERCOT**	**HQ**	Units
Max. Delta Frequency (MDF)	**0.420**	**0.280**	**0.405**	**0.947**	
Resource Loss Protection Criteria (RLPC)[1]	**3,209**	**2,850**	**2,750**	**2,000**	MW
Credit for Load Resources (CLR)			**1,209**		MW
Current IFRO (OY 2018)	**-1,015**	**-858**	**-381**	**-179**	MW/0.1 Hz
First-Step target IFRO[1]	**-915**	**-1018**	**-380**	**-211**	MW/0.1 Hz
Second-Step target IFRO[1, 2]	**-815**				
Final target IFRO[1, 2]	**~~-784~~ -787**				

Table 1: Interconnection Frequency Response Obligations (base year 2017)

IFRO = (RLPC – CLR)/Max Delta Freq/10

1. *These values are evaluated annually for changes in each Interconnection.*
2. *To reduce risk, the Eastern Interconnection IFRO will be stepped down annually from the 2017 value of -1,015 MW/0.1 Hz in -100 MW/0.1 Hz increments. If during the step down process, Interconnection Frequency Response Measure (FRM) declines by more than 10 percent, the ERO will halt the reduction in IFRO until such time that a determination can be made as to the cause of the degradation.*

Balancing Authority Frequency Response Obligation and Frequency Bias Setting

For a multiple Balancing Authority interconnection, the Interconnection FRO shown in Table 1 is allocated based on the Balancing Authority annual load and annual generation. The FRO allocation will be based on the following method:

$$\text{FRO}_{\text{BA}} = \text{IFRO} \quad \times \frac{\text{Annual Gen}_{\text{BA}} + \text{Annual Load}_{\text{BA}}}{\text{Annual Gen}_{\text{Int}} + \text{Annual Load}_{\text{Int}}}$$

Where:

- Annual Gen_{BA} is the total annual output of generating plants within the Balancing Authority Area (BAA).
- Annual Load_{BA} is total annual Load within the BAA.
- Annual Gen_{Int} is the sum of all Annual Gen_{BA} values reported in that interconnection.
- Annual Load_{Int} is the sum of all Annual Load_{BA} values reported in that interconnection.

Balancing Authorities that elect to form a FRSG will calculate a FRSG FRO by adding together the individual BA FRO's.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_{A} and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Submit a joint Form 1 with the "FRSG" tab completed for the aggregate performance of the participating Balancing Authorities.

Balancing Authorities that merge or transfer load or generation are encouraged to notify the ERO of the change in footprint and corresponding changes in allocation such that the net obligation to the Interconnection remains the same and so that CPS limits can be adjusted.

Each Balancing Authority reports its previous year's FRM, Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO each year to allow the ERO to validate the revised Frequency Bias Settings on FRS Form 1. In addition, each Balancing Authority will report its two largest potential resource losses and any applicable N-2 RAS events in the form. If the ERO posts the official list of events after the date specified in the timeline below, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1.

Once the ERO reviews the data submitted in FRS Form 1 and FRS Form 2 for all Balancing Authorities, the ERO will use FRS Form 1 data to post the following information for each Balancing Authority for the upcoming year:

- Frequency Bias Setting
- Frequency Response Obligation (FRO)

Once the data listed above is fully posted, the ERO will announce the three-day implementation period for changing the Frequency Bias Setting if it differs from that shown in the timeline below.

A Balancing Authority using a fixed Frequency Bias Setting sets its Frequency Bias Setting to the greater of (in absolute value):

- Any number the Balancing Authority chooses between 100 percent and 125 percent of its Frequency Response Measure as calculated on FRS Form 1
- Interconnection Minimum as determined by the ERO

For purposes of calculating the minimum Frequency Bias Setting, a Balancing Authority participating in a FRSG will need to calculate its stand-alone FRM using FRS Form 1 and FRS Form 2 to determine its minimum Frequency Bias Setting.

A Balancing Authority providing Overlap Regulation will report the historic peak demand and generation of its combined Balancing Authorities' areas on FRS Form 1 as described in Requirement R4.

Frequency Response Measure

The Balancing Authority will calculate its FRM from Single Event Frequency Response Data (SEFRD), defined as: "the data from an individual event in a Balancing Authority area that is used to calculate its Frequency Response, expressed in MW/0.1Hz" as calculated on FRS Form 2 for each event shown on FRS Form 1. The events in FRS Form 1 are selected by the ERO using the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*. The SEFRD for a typical Balancing Authority in an Interconnection with more than one Balancing Authority is the change in its Net Actual Interchange on its tie lines with adjacent Balancing Authorities divided by the change in Interconnection frequency. Some Balancing Authorities may choose to apply corrections to their Net Actual Interchange (NA_I) values to account for factors such as nonconforming loads. FRS Form 1 and 2 shows the types of adjustments that are allowed. Note that with the exception of the Contingent BA column, any adjustments made must be made for all events in an evaluation year.[1]

The ERO will use a standardized sampling interval of approximately 16 seconds before the event, up to the time of the event for the pre-event NA_I, and frequency (A values), and approximately 20 to 52 seconds after the event for the post-event NA_I (B values) in the computation of SEFRD values, dependent on the data scan rate of the Balancing Authority's Energy Management System (EMS).

All events listed on FRS Form 1 need to be included in the annual submission of FRS Forms 1 and 2. The only time a Balancing Authority should exclude an event is if its tie-line data or its Frequency data is corrupt, or its EMS was unavailable. FRS Form 2 has instructions on how to

[1] As an example, if an entity has non-conforming loads and makes an adjustment for one event, all events must show the non-conforming load, even if the non-conforming load does not impact the calculation. This ensures that the reports are not utilizing the adjustments only when they are favorable to the BA.

correct the BA's data if the given event is internal to the BA or if other authorized adjustments are used.

Assuming data entry is correct, FRS Form 1 will automatically calculate the Balancing Authority's FRM for the past 12 months as the median of the SEFRD values. A Balancing Authority electing to report as an FRSG or a provider of Overlap Regulation Service will provide an FRS Form 1 for the aggregate of its participants.

To allow Balancing Authorities to plan its operations, events with a "Point C" that cause the Interconnection Frequency to be lower than that shown in Table 1 above (for example, an event in the Eastern Interconnection that causes the Interconnection Frequency to go to 59.4 Hz) or higher than an equal change in frequency going above 60 Hz may be included in the list of events for that Interconnection. However, the calculation of the Balancing Authority response to such an event will be adjusted to show a frequency change only to the Target Minimum Frequency shown in Table 1 above (in the previous example this adjustment would cause Frequency to be shown as 59.5 Hz rather than 59.4 HZ) or a high frequency amount of an equal quantity. Should such an event happen, the ERO will provide additional guidance.

Balancing Authorities that elect to form a FRSG as a means to jointly meet the FRO will calculate their FRM performance one of two ways:

- Calculate a group NI_A and measure the group response to all events in the reporting year on a single FRS Form 1, or
- Jointly submit the individual Balancing Authority's Form 1s, with a summary spreadsheet that contains the sum of each participant's individual event performance.

Timeline for Balancing Authority Frequency Response and Frequency Bias Setting Activities

Described below is the timeline for the exchange of information between the ERO and Balancing Authorities to:

- Facilitate the assignment of Balancing Authority FRO
- Calculate Balancing Authority FRM
- Determine Balancing Authority Frequency Bias Settings

Target Business Date	Activity
March 1	**FRS Form 1 is posted by the ERO* with all selected events for the operating year for BA usage.**
April 1	**BAs and FRSGs complete their frequency response forms for all four quarters, including the BAs' FBS calculations, returning the results to the ERO.**
May 1	**The ERO validates FBS values, computes the sum of all FBS values for each Interconnection.**
May 15	**The BAs not required to file FERC Form 714 receive a request to provide load and generation data as described in the *Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*** **to support FRO assignments and determining minimum FBS for the upcoming year. Data to be provided by July 15.**
June 1	The BA implements any changes to their FBS.
November 1	The ERO assigns FRO values and Minimum FBS for the upcoming year to the BAs.

* If 4th quarter posting of FRS Form 1s is delayed, the ERO may adjust the other timelines in this table by a similar amount.

** Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

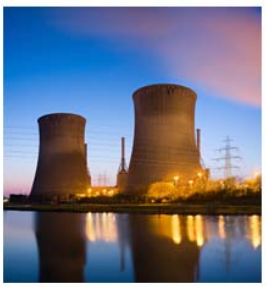
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 8(iii)
Standards Committee
December 18, 2019

Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard

Version II - 2019

RELIABILITY | RESILIENCE | SECURITY

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

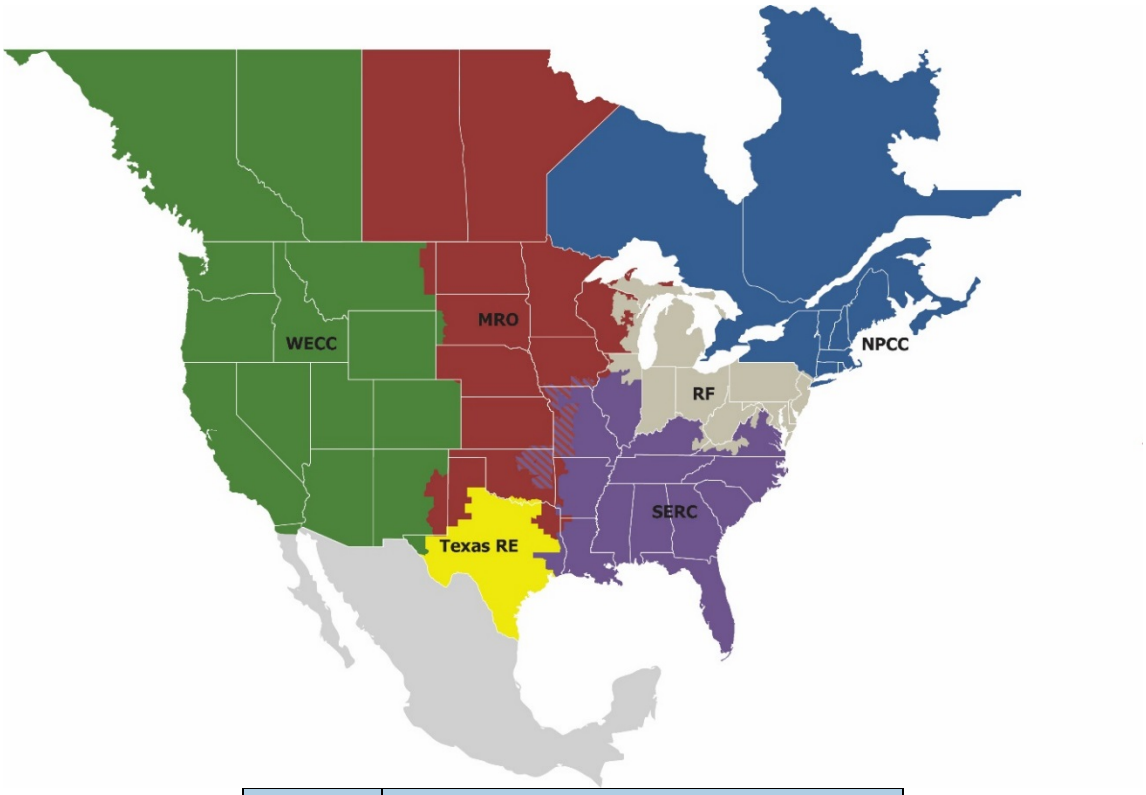
Table of Contents

Preface

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

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

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



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

Introduction

This procedure (Procedure) outlines the Electric Reliability Organization (ERO) process for supporting the Frequency Response Standard (FRS). A request for revisions may be submitted to the ERO or its designee for consideration. The request must provide a technical justification for the suggested modification. The ERO shall publicly post the suggested modification for a 45-day formal comment period and discuss the request in a public meeting. The ERO will make a recommendation to the NERC Board of Trustees (BOT), which may adopt the revision request, reject it, or adopt it with modifications. Any approved revision to this Procedure shall be filed with the Federal Energy Regulatory Commission (FERC) for informational purposes.

BAL-003-2 sets Interconnection Frequency Response Obligation (IFRO) to preset values subject to annual review. This procedure establishes the methods to be used for the annual review until Phase 2 of the SAR for Project 2017-01 has been addressed. If Frequency Response Measure (FRM) for the Eastern Interconnection degrades more than 10% in a year, the ERO will halt the reduction in IFRO until such time as a determination can be made as to the cause of the degradation.

Chapter 1: Event Selection Process

Event Selection Objectives

The goals of this procedure are to outline a transparent, repeatable process to annually identify a list of frequency events to be used to calculate Frequency Response to determine:

- Whether the Balancing Authority (BA) or Frequency Response Sharing Group (FRSG) met its Frequency Response Obligation, and
- An appropriate fixed Frequency Bias Setting.

Event Selection Criteria

1. The ERO will use the following criteria to select FRS excursion events for analysis. The events that best fit the criteria will be used to support the FRS. The evaluation period for performing the annual Frequency Bias Setting and the FRM calculation is December 1 of the prior year through November 30 of the current year.
2. The ERO will identify 20 to 35 frequency excursion events in each Interconnection for calculating the Frequency Bias Setting and the FRM. If the ERO cannot identify 20 frequency excursion events in a 12-month evaluation period satisfying the criteria below, then similar acceptable events from the previous year's evaluation period will be included with the data set by the ERO for determining compliance.
3. The ERO will use three criteria to determine if an acceptable frequency excursion event for the FRM has occurred:
    a. The change in frequency as defined by the difference from the A Value to Point C and the arrested frequency Point C exceeds the excursion threshold values specified for the Interconnection in Table 1 below.
        i. The A Value is computed as an average over the period from -16 seconds to 0 seconds before the frequency transient begins to decline.
        ii. Point C is the arrested value of frequency observed within 20 seconds following the start of the excursion.

Table 1.1: Interconnection Frequency Excursion Threshold Values

Interconnection	A Value to Pt C	Point C (Low)	Point C (High)
East	0.04Hz	< 59.96	> 60.04
West	0.07Hz	< 59.95	> 60.05
ERCOT	0.08Hz	< 59.92	> 60.08
HQ	0.30Hz	< 59.85	> 60.15

    b. The time from the start of the rapid change in frequency until the point at which Frequency has stabilized within a narrow range should be less than 20 seconds.
    c. If any data point in the B Value average recovers to the A Value, the event will not be included.
4. Pre-disturbance frequency should be relatively steady and near 60.000 Hz for the A Value. The A Value is computed as an average over the period from -16 seconds to 0 seconds before the frequency transient

begins to decline. For example, given the choice of the two events below, the one on the right is preferred as the pre-disturbance frequency is stable and also closer to 60 Hz.

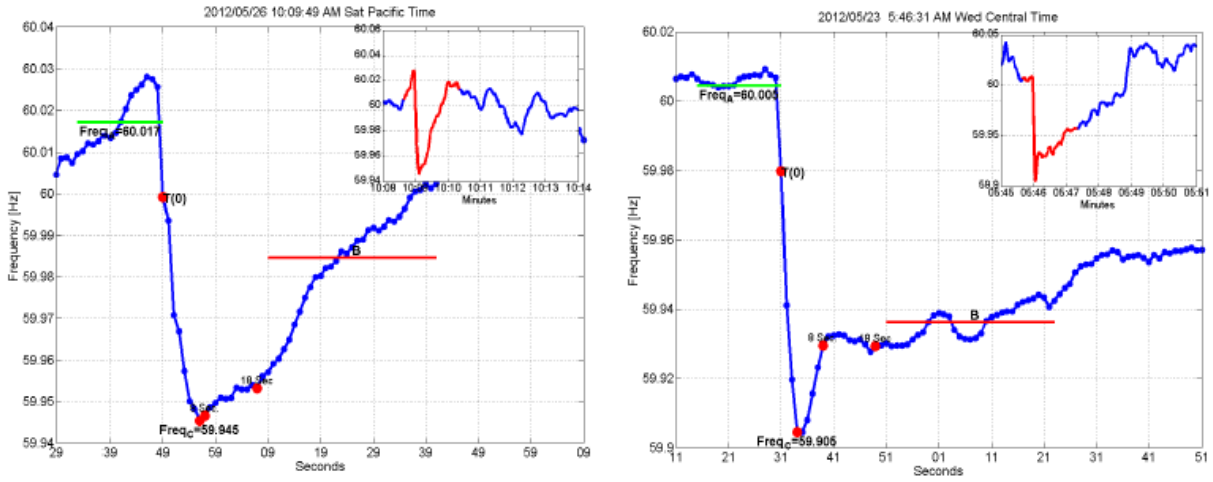


Figure 1.1: Pre-disturbance Frequency

5. Excursions that include 2 or more events that do not stabilize within 20 seconds will not be considered.
6. Frequency excursion events occurring during periods when large interchange schedule ramping or load change is happening, or within 5 minutes of the top of the hour may be excluded from consideration if other acceptable frequency excursion events from the same quarter are available.
7. The ERO will select the largest (A Value to Point C) 2 or 3 frequency excursion events occurring each month. If there are not 2 frequency excursion events satisfying the selection criteria in a month, then other frequency excursion events should be picked in the following sequence:
   a. From the same event quarter of the year.
   b. From an adjacent month.
   c. From a similar load season in the year (shoulder vs. summer/winter)
   d. The largest unused event.

As noted earlier, if a total of 20 events are not available in an evaluation year, then similar acceptable events from the next year's evaluation period will be included with the data set by the ERO for determining Frequency Response Obligation (FRO) compliance. The first year's small set of data will be reported and used for Bias Setting purposes, but compliance evaluation on the FRO will be done using a 24-month data set.

To assist Balancing Authority preparation for complying with this standard, the ERO will provide quarterly posting of candidate frequency excursion events for the current year FRM calculation. The ERO will post the final list of frequency excursion events used for standard compliance as specified in Attachment A of the standard. The following is a general description of the process that the ERO will use to ensure that BAs can evaluate events during the year in order to monitor their performance throughout the year.

Quarterly

The event lists will be reviewed quarterly, with the quarters defined as:

- December through February
- March through May
- June through August
- September through November

Based on criteria established in this Procedure, events will be selected to populate the FRS Form 1 for each Interconnection. The FRS Form 1's will be posted on the NERC website, in the Resources Subcommittee (RS) area under the title "Frequency Response Standard Resources". Updated FRS Form 1's will be posted at the end of each quarter listed above after a review by the NERC RS and its Frequency Working Group. While the events on this list are expected to be final, as outlined in the selection criteria, additional events may be considered, if the number of events throughout the year do not create a list of at least 20 events. It is intended that this quarterly posting of updates to the FRS Form 1 would allow BAs to evaluate the events throughout the year, lessening the burden when the yearly posting is made.

Annually

The final FRS Form 1 for each Interconnection, which would contain the events from all four quarters listed above, will be posted as specified in Attachment A. Each BA reports its previous year's Frequency Response Measure (FRM), Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO as specified in Attachment A using the final FRS Form 1. The ERO will check for errors and use the FRS Form 1 data to calculate CPS limits and FROs for the upcoming year.

Once the data listed above is fully reviewed, the ERO may adjust the implementation specified in Attachment A for changing the Frequency Bias Settings and CPS limits. This allows flexibility when each BA implements its settings.

Chapter 2: Process for Adjusting Interconnection Minimum Frequency Bias Setting

This procedure outlines the process the ERO is to use for modifying minimum Frequency Bias Settings to better meet reliability needs. The ERO will adjust the Frequency Bias Setting minimum in accordance with this procedure.
The ERO will post the minimum Frequency Bias Setting values on the ERO website along with other balancing standard limits.

Under BAL-003-2, the minimum Frequency Bias Settings will be moved toward the natural Frequency Response in each Interconnection. In the first year, the minimum Frequency Bias Setting for each Interconnection is shown in Table 2 below. Each Interconnection Minimum Frequency Bias Setting is based on the sum of the non-coincident peak loads for each BA from the currently available FERC 714 Report or equivalent. This non-coincident peak load sum is multiplied by the percentage shown in Table 2 to get the Interconnection Minimum Frequency Bias Setting. The Interconnection Minimum Frequency Bias Setting is allocated among the BAs on an Interconnection using the same allocation method as is used for the allocation of the Frequency Response Obligation (FRO).

Table 2.1: Frequency Bias Setting Minimums

Interconnection	Interconnection Minimum Frequency Bias Setting (in MW/0.1Hz)
Eastern	0.9% of non-coincident peak load
Western	0.9% of non-coincident peak load
ERCOT	N/A
HQ	N/A

*The minimum Frequency Bias Setting requirement does not apply to a Balancing Authority that is the only Balancing Authority in its Interconnection. These Balancing Authorities are solely responsible for providing reliable frequency control of their Interconnection. These BAs are responsible for converting frequency error into a megawatt error to provide reliable frequency control, and the imposition of a minimum bias setting greater than the magnitude the Frequency Response Obligation may have the potential to cause control system hunting, and instability in the extreme.

The ERO, in coordination with the regions of each Interconnection, will annually review Frequency Bias Setting data submitted by BAs. If an Interconnection's total minimum Frequency Bias Setting exceeds (in absolute value) the Interconnection's total natural Frequency Response by more (in absolute value) than 0.2 percentage points of peak load (expressed in MW/0.1Hz), the minimum Frequency Bias Setting for BAs within that Interconnection may be reduced (in absolute value) in the subsequent years FRS Form 1 based on the technical evaluation and consultation with the regions affected by 0.1 percentage point of peak load (expressed in MW/0.1Hz) to better match that Frequency Bias Setting and natural Frequency Response.

The ERO, in coordination with the regions of each Interconnection, will monitor the impact of the reduction of minimum frequency bias settings, if any, on frequency performance, control performance, and system reliability. If unexpected and undesirable impacts such as, but not limited to, sluggish post-contingency restoration of frequency to schedule or control performance problems occur, then the prior reduction in the minimum frequency bias settings may be reversed, and/or the prospective reduction based on the criterion stated above may not be implemented.

Chapter 3: Interconnection Frequency Response Obligation Methodology

The Interconnection Resource Loss Protection Criteria (RLPC) is calculated based a resource loss in accordance with the following process:

NERC will request BAs to provide their two largest resource loss values and largest resource loss due to an N-1 or N-2 RAS event. This will facilitate comparison between the existing Interconnection RLPC values and the RLPC values in use. This data submission will be needed to complete the calculation of the RLPC and IFRO.

BAs determine the two largest resource losses for the next operating year based on a review of the following items:

- The two largest independent Balancing Contingency Events, each due to a single contingency, identified using system models measured by megawatt loss in a normal system configuration (N-0). (An abnormal system configuration is not used to determine the RLPC.)
- The two largest units in the BA Area, regardless of shared ownership/responsibility.
- The two largest Remedial Action Scheme (RAS) resource losses (if any) which are initiated by single (N-1) contingency events.

The BA provides these two numbers determined above as Resource Loss A and Resource Loss B in the FR Form 1.

The BA should then provide the largest resource loss due to RAS operations (if any) which is initiated by a multiple contingency (N-2) event (RLPC cannot be lower than this value). If this RAS impacts more than a single BA, one BA is asked to take the lead and sum all resources lost due to the RAS event and provide that information.

The calculated RLPC should meet or exceed any credible N-2 resource loss event.

The host BA (or planned host BA) where jointly-owned resources are physically located, should be the only BA to report that resource. The full ratings of the resource, not the fractional shares, should be reported.

Direct-current (DC) ties to asynchronous resources (such as DC ties between Interconnections, or the Manitoba Hydro Dorsey bi-pole ties to their northern asynchronous generation) should be considered as resource losses. DC lines such as the Pacific DC Intertie, which ties two sections of the same synchronous Interconnection together, should not be reported. A single pole block with normal clearing in a monopole or bi-pole high-voltage direct current system is a single contingency.

For a hypothetical four-BA Interconnection, Plant 1, in BA1, has two generators rated at 1200 MW each. Plant 2, in BA2 has a generator rated at 1400 MW. BA2's next largest contingency is 1000 MW. The two largest resource losses for BA3 and BA4 are listed below.

BA1	Resource Loss A = 1200 MW	Resource Loss B = 1200 MW	Both at Plant 1 (N-2)
BA2	Resource Loss A= 1400 MW	Resource Loss B = 1000 MW	Electrically separate
BA3	Resource Loss A = 1000 MW	Resource Loss B = 800 MW	Electrically separate
BA4	Resource Loss A = 1500 MW (DC TIE)	Resource Loss B = 500 MW	Electrically separate

The ERO would apply the RLPC selection methodology described above to determine the RLPC for the Interconnection. Using this methodology, results in the following:

Largest Resource Loss = 1500 MW
Second Largest Resource Loss = 1400 MW
Summation of two largest resource losses = 2900 MW
Interconnection RLPC = 2900 MW

If only the N-2 Event was applied, the RLPC for the Interconnection would be 2400 MW. The summation of the two largest Interconnection Resource Losses will equal or exceed, but never fall short of, the N-2 Event scenario.

In order to evaluate RAS resource loss, single (N-1) and multiple (N-2) contingency events should be evaluated. Hypothetically, in an Interconnection:

BA1 RAS = 2850 MW N-2 RAS event
BA1 Resource Loss A = 1150 MW
BA1 Resource Loss B = 800 MW
BA2 Resource Loss A = 1380 MW
BA2 Resource Loss B = 1380 MW
BA3 RAS = 1000 MW N-1 RAS event
BA3 Resource Loss A = 800 MW
BA3 Resource Loss B = 700 MW

In this case, the ERO would determine the RLPC as follows: the summation of the two largest resource losses is 2760 MW. Since the N-2 RAS event exceeds the summation of the two largest single contingency events, the RLPC is the N-2 RAS event, or 2850 MW.

Interconnection RLPC Values

Based on initial review, the numbers below would be representative of the RLPC for each Interconnection.

Eastern Interconnection:
Present RLPC = 4500 MW Load Credit = 0 MW
RESOURCE LOSS A = 1732 MW
RESOURCE LOSS B = 1477 MW
Proposed RLPC = 3209 MW

Western Interconnection:
Present RLPC = 2626 MW Load Credit = 0 MW
RESOURCE LOSS A = 1505 MW
RESOURCE LOSS B = 1344 MW
N-2 RAS = 2850 MW
Proposed RLPC = 2850 MW

ERCOT:
Present RLPC = 2750 MW Load Credit = 1209 MW
RESOURCE LOSS A = 1375 MW
RESOURCE LOSS B = 1375 MW
Proposed RLPC = 2750 MW

Quebec Interconnection:
Present RLPC = 1700 MW Load Credit = 0 MW
RESOURCE LOSS A = 1000 MW
RESOURCE LOSS B = 1000 MW
Proposed RLPC = 2000 MW

Calculation of IFRO Values

The IFRO is calculated using the RLPC (reference is from Table 1 from BAL-003-2):

$$IFRO = \frac{(RLPC - CLR)}{(MDF * 10)}$$ expressed as MW/0.1Hz

MDF is the Maximum Delta Frequency for the specific interconnection as determined in the 2017 Frequency Response Annual Analysis (FRAA).

Interconnection Frequency Response Obligation

Interconnection	Eastern	Western	ERCOT	HQ	Units
Max. Delta Frequency (MDF)	**0.420**	**0.280**	**0.405**	**0.947**	Hz
Resource Loss Protection Criteria (RLPC)	**3,209**	**2,850**	**2,750**	**2,000**	MW
Credit for Load Resources (CLR)			**1,209**		MW
Calculated IFRO	**~~-784~~787***	**-1018**	**-380**	**-211**	MW/0.1Hz

* Eastern Interconnection IFRO will be stepped down to this level over three years per BAL-003-2.

SER Evidence Retention Recommendations

Action

Endorse the recommendations below made by the Standards Efficiency Review sub-team in its Evidence Retention white-paper.

Summary

The SER evidence retention sub-team simplified the existing evidence retention schemes. The recommended set of five evidence retention schemes covers all NERC Operations & Planning and Critical Infrastructure Protection (CIP) Reliability Standards and requirements as shown in the following table.

Recommended Data/Evidence Retention Schemes	Rationale for the Data/Evidence Retention Scheme
1. Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review. If revised within the last year, the prior version should also be retained.	This satisfies the need for auditors to see the most recent documentation in a variety of areas. What is most important is the current document and that document should have a revision history showing that it is regularly reviewed and updated. In some instances, evidence retention may exceed a three year period.
2. Most recent full testing records with evidence of previous testing intervals.	This satisfies the requirements to complete and document various tests and includes the requirement to have evidence of the previous full testing records. In some instances, evidence retention may exceed a three-year period.
3. Rolling 3 Months data retention period.	Data retention schemes that require significant computer storage, such as voice and audio recordings, could be reduced to 3 months of rolling history.
4. Rolling 12 Months data retention period.	This satisfies existing evidence retention scheme requirements that have at least 12 months of data. Based on the type of data or reliability risk, it may not be necessary to retain 36 months of data.
5. Rolling 36 Months data retention period.	Many existing evidence retention schemes call for a three-year (36-month) retention schedule. The 36-month data retention is retained with the addition of “rolling”.

Recommended Actions

The SER Phase 2 team Data/Evidence Retention Project team recommends the following actions:

1. Consider Rules of Procedure (ROP) changes for evidence retention to minimize administrative burden. (NERC staff)

2. Retire Compliance Bulletin #2011-001 Data Retention Requirements, once ROP changes are in effect or publish CMEP guidance to supersede the bulletin. (ERO Enterprise staff and CCC)
3. Concurrent to ROP changes, update standard drafting teams (SDTs) references and notify active SDTs, with the minimum options for risk-based data retention schemes, as described above. In addition, the headings within Reliability Standard should be consistently named "Data and Evidence Retention Period". (Standards Committee (SC))
4. If desired, concurrent with ROP changes, establish a project to revise evidence retention schemes for enforceable Reliability Standards with a standard drafting team, Periodic Review team, or other mechanism. (SC, CCC, and NERC staff)
5. Ensure changes to CMEP evidence retention processes are made in associated documents and communicated with ERO Enterprise staff, such as NERC Auditor's Manual, training materials, etc. (NERC staff)
6. Ensure final recommendations of SER Evidence Retention are circulated with the CCC, SC, and NERC staff, and recommendations are incorporated into respective work plans in 2020. (CCC, SC, NERC staff)

Standard Efficiency Review (SER) Phase 2
Evidence Retention Team's Recommended
Evidence Retention Schemes

Evidence and Data Retention White Paper

Analysis and Recommendations

11/14/2019

Puscas, Michael, ISO-NE
Zaragoza, Tino, IID
Bilke, Tery, MISO

Table of Contents

Contents

Executive Summary

This document analyzes the evidence or data retention sections of NERC CIP and O&P Standards as part of the NERC Standards Efficiency Review (SER) Phase 2 Project.[1]

Executive Summary

The Rules of Procedure (ROP) of the North American Electric Reliability Corporation (NERC), dated July 19, 2018, indicates:

> **"All Bulk Power System owners, operators, and users shall provide to NERC and the applicable Regional Entity such information as is necessary to monitor compliance with the Reliability Standards. NERC and the applicable Regional Entity will define the data retention and reporting requirements in the Reliability Standards and compliance reporting procedures."**[2]

The ROP indicates how long evidence should be retained by Compliance Enforcement Authorities (CEA), but the amount of time evidence must be retained by registered entities gets more complicated. There are over 50 evidence retention schemes in the existing set of NERC Operation and Planning (O&P) and CIP Standards (see Appendix A). Many evidence retention schemes apply to only one requirement in one Standard.

This is not a new or unknown problem. NERC and an associated study team produced a "Data Retention White Paper", dated September 12, 2014[3]. This document described a research and analysis project that started in 2013 when the Electric Reliability Organization (ERO) Enterprise assembled an advisory group to provide input and advice for modification of existing NERC Reliability Standard data retention requirements. The data retention team was comprised of representatives from NERC and the NERC Compliance and Certification Committee (CCC).

The 2014 data retention study team began reviewing and analyzing current data retention requirements and soliciting industry feedback on current data retention requirements. Their subsequent white paper presented their findings and made recommendations for changes to current guidance documents, future NERC Reliability Standard development, and auditing processes.

The white paper's analysis explored possible options for establishing uniform tools and applications and standardizing evidence retention requirements across the ERO Enterprise to promote consistency in demonstrating compliance. These options were intended to provide improvements that support reliability and ensure that resources allocated by the ERO Enterprise and registered entities are commensurate with the potential risks of noncompliance to reliability.

The 2014 white paper recommended that NERC modify data retention requirements so that the burden of producing records necessary to demonstrate compliance is commensurate with the risk to the reliability of the BPS. It further recommended including a consistent data retention period of either a rolling 6-months for high-volume data[4], or a 4-year retention period for all other data, with two specific exceptions:

1. Standards requiring a current program or procedure, which would be limited to the currently effective version with a revision history specifying changes and dates of review; and

[1] Author: Dr. Michael Puscas, Ed.D., Compliance Manager, ISO-NE. Reviewer: Tino Zaragoza, Reliability Compliance Officer, Imperial Irrigation District

[2] NERC Rules of Procedure Link, see pg. 22, #3; pg. 27, #3; and Section 9.0, pg. 29

[3] Data Retention White Paper - 2014

[4] "High-volume data," as used herein, refers to electronic data sets and files, paper documents, or audio recordings with sizes making it cost- or space-prohibitive to gather, maintain, track, and provide the data to auditors within a reasonable period. Examples of high-volume data could be access logs, video surveillance tapes, or voice and telephone recordings.

2. Standards requiring testing at intervals, which would require the retention of the last full testing record and evidence of recurrence.

The white paper recommended simplifying data requests by including as a part of the ERO Compliance Auditor Manual and Handbook a recommendation that, regardless of the data retention requirements of the Standard and time between Compliance Audits, auditors focus sampling to the most recent two years. This recommended method of sampling would be more efficient and less burdensome for registered entities and the ERO Enterprise. By instituting the recommended method of sampling, the ERO Enterprise and registered entities could reallocate resources to areas of greater risk to the reliability of the BPS.

The recommendations contained in the 2014 white paper were presented to NERC and the Standards Committee, but not fully implemented. Data and evidence retention schemes remain overly complicated and burdensome. The Standards Efficiency Review (SER) Phase 2 team recognized that data and evidence retention issues remain and require attention. The SER Phase 2 team continued the work of the 2014 team.

The evidence retention team once again analyzed the current evidence retention schemes in the current set of O&P and CIP mandatory standards. They discovered over 50 different evidence retention schemes (see Appendix A). They sorted the list of requirements by VRF (see Appendix B) and they prepared a draft set of five new and simplified evidence retention schemes. The evidence retention team proposed a new evidence retention scheme for each NERC Standard requirement based on the risk to the BES (see Appendix D).

The remainder of this report presents five new and simplified data retention schemes along with their justification. It also recommends new data retention schemes for high VRF requirements. More information is contained in the following sections:

Revision History

Date	Version	Description
06/13/2019	0.1	First Draft
06/24/2019	0.2	Second Draft
10/11/2019	0.3	Third Draft, incorporate comments from industry
11/14/2019	0.4	Fourth Draft, incorporate comments from NERC staff
TBD	1.0	Final Draft and Initial release of the Evidence Retention Report.

Overview - SER Phase 2 Overview

This portion of the evidence retention report summarizes the SER Phase 2 Project.

Overall SER Project Scope

Evaluate NERC Reliability Standards using a risk-based approach to identify potential efficiencies through retirement or modification of Reliability Standard Requirements. Considering that many Reliability Standards have been mandatory and enforceable for 10+ years in North America, this project seeks to identify potential candidate requirements that are not essential for reliability, could be simplified or consolidated, and could thereby reduce regulatory obligations and/or compliance burden.[5]

SER Phase 2: Evidence Retention Project Scope

Evaluate NERC Reliability Standards (O&P and CIP), as informed by implementation experiences and compliance practices, to develop and recommend standards-based solutions intended to reduce inefficiencies and unnecessary regulatory burdens for the purpose of supporting continued safe, secure and reliable operations. The Phase Two Team will focus on the following activities:

- Identify areas of inefficiency in the current framework of Reliability Standards
- Collaborate and communicate with industry to ensure all areas of inefficiency and potential solutions are considered
- Potential solutions may include, but are not limited to the following:
    - SARs to remove inefficiencies in the Reliability Standards
    - Policy recommendations to appropriate ERO staff or committee[6]

SER Phase 2 Efficiency Concepts[7]

The SER Phase 2 team identified six efficiency concepts including:

1. **Evidence Retention Overhaul**
2. Prototype Standard
3. Move Requirements to Guidance
4. Consolidate and Simplify Training Requirements
5. Consolidate Information/Data Exchange Requirements
6. Relocate Competency-based Requirements to Certification Program/CMEP Controls Review

The SER Phase 2 team surveyed the industry through a questionnaire that concluded on March 22, 2019. The highest rated efficiency concept was Evidence Retention. The results were presented to the SER Phase 2 Advisory Group. NERC, in concert with the Advisory Group, examined industry comments both for and against the concept (see below). Together they determined that the Evidence Retention concept would become the first priority for the SER Phase 2 team since work was completed in 2014 and the SER team could build on that work.

[5] https://www.nerc.com/pa/Stand/Pages/Standards-Efficiency-Review.aspx
[6] Ibid
[7] SER Phase 2 Concepts 2-6 are outside the scope of this document. Please refer to SER web page: https://www.nerc.com/pa/Stand/Pages/Standards-Efficiency-Review.aspx

Summary of the 2014 Evidence Retention Project

Analysis of 2014 Evidence Retention White Paper

The SER Phase 2 Evidence Retention team began by reviewing and analyzing the work of the 2014 project team (see Objectives) to avoid unnecessary duplication of effort, and to validate or repudiate the recommendations by that project team.

Tasks Performed by the 2014 Evidence Retention Team

The 2014 Evidence Retention team began reviewing and analyzing the data retention requirements in the then currently-enforceable and NERC Board of Trustee approved NERC Reliability Standards, the NERC Rules of Procedure, and guidelines for auditing included in the Generally Accepted Government Auditing Standards (GAGAS). Finally, the data retention team reviewed the ERO Enterprise Compliance Auditor Manual and Handbook (Auditor Manual). They completed the following tasks:

- Identified and evaluated data retention requirements in the then current NERC Standards;
- Recommended improvements to reduce the data-maintenance burdens on registered entities;
- Provided guidance regarding the levels of data necessary to support proof of compliance;
- Recommended revised data retention requirements to be commensurate with risk to the BPS; and
- Recommended methods of sampling that are more efficient and less burdensome for registered entities.

Purpose of the 2014 White Paper

The 2014 Evidence Retention study team created a "White Paper" to present their findings. The twofold purpose of the evidence retention white paper was to provide rationale for proposed revisions to:

1. The data retention requirements in NERC Reliability Standards; and
2. The methodology of Compliance Audit and Spot Check data sampling requests.

The goal was to minimize the Compliance Enforcement Authority (CEA) and registered entity resources used for gathering, storing, and producing data while maintaining reasonable assurance of compliance with the effective NERC Reliability Standards and reliability of the BPS.

Identified Evidence Retention Problems, Issues and Concerns

The 2014 Evidence Retention team examined the data retention requirements of each active NERC Standard[8]. The 2014 team identified a series of data retention problems, for example, as noted in their white paper:

- There is no current consistent data retention period prescribed by FERC (the Commission) or NERC applicable to all Reliability Standards. For example:
    - BAL-001-0.1a requires a one-year retention period for real-time operating data
    - VAR-002-2b requires two years of real-time operating data
    - COM-001-1.1 requires a 90-day retention of operator logs.
    - IRO-006-5, if the records are audio recordings, they have a 90-day retention but if documented transcripts then it should be 12 months

[8] **NOTE**: Many NERC Standards that were active in 2014 are now either inactive or replaced by newer versions.

    - MOD-028-2 requires retaining data for 12 months for seven of its requirements, but either 14, 30, or 60 days for two other requirements
- There are different requirements for the length of time registered entities must keep identical types of data for certain Reliability Standards.
- The ERO Enterprise has considerable flexibility to determine and identify how long a registered entity must retain evidence to show compliance.
- Current evidence retention policies aren't related to high reliability risk areas and therefore places undue administrative burden on registered entities.
- The NERC Rules of Procedure (ROP)[9] do not include specific evidence retention guidance for registered entities. The Rules of Procedure leave the assignment of data retention and reporting requirements to NERC or the Regional Entity.
- Industry responses voiced a frustration and opinion that the focus of auditor data requests and NERC Reliability Standards data retention requirements are on proving compliance and not enhancing reliability. They voiced a desire to focus on current practices and policies instead of historical documents, which may not have been relevant for several years.

Recommendations from the 2014 Evidence Retention Study Team's White Paper

The 2014 Evidence Retention team documented a series of recommendations:

- NERC should modify data retention requirements in Standards so that the burden of producing records necessary to demonstrate compliance is commensurate with the impact to the reliability of the BPS.
- All new Standards receive a default four-year data retention period. This four-year period will exclude the following:
    - Voice and audio recordings, which will continue to be a 90-day rolling retention period.
    - High-volume data, which would be restricted to a six-month rolling retention period.
    - Standards requiring a current program or procedure, which would restrict to the currently effective version with a revision history specifying changes and dates of review.
    - Standards requiring testing intervals (e.g. PRC-005), which would restrict to the most recent full testing records with evidence of previous testing intervals.
- If current Reliability Standards are silent as to a data retention period, then the four-year or six-month data retention period should be used.
- Data sampling by CEAs should be focused on the most recent two years, unless the data sample would be statistically too small or irregularities are identified in the initial samples.

[9] https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20180719.pdf

2019 SER Phase 2 Evidence Retention Project Overview

Introduction to SER Phase 2 Evidence Retention Project

This project evaluates and continues the work completed by the 2014 Evidence Retention team. NERC conducted a survey to gather industry comments related to six efficiency concepts. Analysis of industry comments indicated that the Evidence Retention concept was the highest rated SER Phase 2 concept. NERC and the SER Advisory Group selected the Evidence Retention concept as the first SER Phase 2 initiative. This will be verified through meetings with the CCC on June 18th, 2019 and with the NERC Standards Committee (SC) on June 26th, 2019.

SER Phase 2 Evidence Retention Project Team

1. Michael Puscas, Evidence Retention Team Lead (ISO-NE)
2. Tino Zaragoza, Evidence Retention Team Co-Lead (IID)
3. Chris Larson, NERC SER Phase 2 Project Lead
4. Amy Casuscelli, SC Vice-Chair
5. Ed Kichline
6. John Allen, SER Phase 2 Project Chair
7. Ryan Mauldin
8. Kiel Lyons
9. Steve Noess
10. Jennifer Flandermeyer, (NERC CCC Chair)
11. Terry Bilke (MISO)

Evidence Retention Project Objectives

The SER Phase 2 Evidence Retention team will:

Objective
1. Review and analyze the 2014 Evidence Retention efforts retaining recommendations that are still appropriate and valid.
2. Inventory and analyze the Evidence Retention schemes in currently enforceable Standards to determine impact on reliability and high risks.
3. Build on the work of the 2014 Evidence Retention team and document a new and much simplified set of data retention guidelines.
4. Recommend and justify proposed data/evidence retention solutions for each high VRF NERC Standard requirement.
5. Determine, in concert with the SER Advisory Committee, NERC CCC, and NERC Management how to implement the recommendations of the Evidence Retention Team and the appropriate committee to oversee the successful implementation of the recommendations.

Evidence Retention Project Scope

The Evidence Retention efficiency project includes:

- Analysis of current mandatory O&P and CIP Standards.
- Analysis of the risk levels of each Standard requirement.
- Analysis of Data and Evidence Retention sections of the NERC Standards.

Evidence Retention Out of Scope

The Evidence Retention efficiency project does not include:

- O&P and CIP Standards subject to future enforcement.
- Auditor compliance evidence sampling methodologies.
- Specific evidence retention implementation plans and strategies.
- Changes to any portion of a given NERC Standard.
- Methods of data/evidence sampling during audits.

Evidence Retention Project Assumptions

The Evidence Retention efficiency project assumes:

- The recommendations of the SER Phase 2 team's recommendations will be assigned to an owner who will assure that the evidence retention recommendations are fully implemented.
- The committee or owner will establish an implementation strategy and timeline for the new evidence retention schemes.

Evidence Retention Questions

The Evidence Retention team considered the following questions:

Questions	Answers
What is the purpose and value of evidence retention?	Data and evidence is important because it provides information to support decision-making by auditors who monitor and enforce compliance with Reliability Standards, and is mandatory to meet regulatory requirements.
How are measures related to evidence retention? Should they be considered as part of this effort? Is it beneficial to have measures in the Standard?	Standard requirement measures often indicate what the specific evidence should look like. The data or evidence retention portion of the Standard explains how long to keep that evidence. The two are somewhat related. Measures describe the tangible artifacts, while the data/evidence retention rules are time-based.
Are there potential benefits if the measures, especially for high Violation Risk Factor requirements, were written differently?	Measures in NERC Standards are already sufficiently detailed to indicate what information needs to be collected. Rewriting them by adding retention information would only create more confusion.
Can we find opportunities to revise the measure language to reduce the burden of collecting, storing, and producing records?	Going forward, as new Standards are developed or existing Standards are revised, it is important to assure that the measures are clearly and specifically written without reference to how long to keep records.
Is it practical to collect the type of evidence mentioned in the requirements and/or measures, if the reliability risk is low?	If the reliability risk is low, then data retention length should be as short as possible.

Questions	Answers
How do we assure people that they don't need to continue to keep evidence forever?	Once the new evidence retention schemes are adopted, Standards are updated, and CEAs are trained, then everyone will be held responsible only for the specific time period mentioned in the Standards.
How do registered entities overcome the fear that entities will be asked for evidence beyond what is stated in the Standard?	Included in the recommendations below, NERC would pursue supporting Rules of Procedure changes to minimize evidence retention obligations of entities. CEAs would thereby obligated to follow the revised ROP.
How do we make sure that we don't go through an SER-Type activity in five years? We need to make sure this is a one-and-done mentality.	The NERC Standards are always in a state of continuous process improvement. There will always be some changes occurring in the NERC Standards, but NERC expects that the SER process if properly implemented will preclude another SER effort in five or more years.
What is the difference between measures and evidence retention? Measures provide descriptions of "what" evidence should be collected. The evidence retention section of the Standard describes how long to keep the collected evidence.	This is detailed in the analytical section of this report starting on page 18.

Benefits of Revised Data Retention Schemes

The advantages of a simplified set of data retention schemes:

- Reduce compliance costs associated with low risk activity by reducing an entity's obligation to retain and manage excessive or unnecessary data/evidence.
- Reduce space on servers, which could be used for other purposes. Excessive data retention increases costs to manage, backup, compile, and review data for compliance monitoring and enforcement activities.
- Enable entities to align their internal retention policies with the NERC requirements and only retain relevant data for the time periods noted to demonstrate compliance.
- Examination of current data/evidence retention schemes incentivizes creative thinking and data retention best practices.
- Data and evidence retention schemes are aligned with risk and reliability.
- Provide long-term stability to the Reliability Standards and it provides clear guidance to SDT's, which can potentially reduce overall Standard development time.

Evidence Retention Project Timeline

Date	Event	Status
5/8/19	Draft Evidence Retention Report Due	Complete
5/13/19	Working Meeting	Complete
5/20/19	Meet with Chris Larson and John Allen	Complete
6/11/19	SER Advisory Committee Meeting in Atlanta, GA	Complete
6/15/19	Second draft of the Evidence Retention Report Due	Complete
6/18/19	John Allen meets with NERC CCC for status update	Complete
6/26/19	Meet with NERC SC	Complete
6/30/19	Third draft of the Evidence Retention Report Due	Complete

7/15/19	Determine who "owns" the Evidence Retention recommendations and implementation process	Complete
9/23/19	Industry Feedback on Evidence Retention draft report due.	Complete
10/4/19	NERC Staff meeting to solidify draft report feedback.	Complete
10/18/19	Draft of the Evidence Retention Report Due	Complete
11/14/19	Revisions based on additional feedback	Complete

Evidence Retention Concept – Industry Comments

This section presents a summary of industry comments for and against the Evidence Retention concept.

Industry Comments in Support of the Evidence Retention Concept

1. Today's practice relies too much on the historical evidence which promulgates the burdensome practices of retaining data for indefinite time periods. There needs to be a revolution in the current thinking of having evidence to document compliance with each and every requirement, to only retain the necessary evidence to demonstrate the reliability intent of a standard. For example, demonstrating reliability, not merely having the record of compliance. Our concern is there have been exceptions to the standard retention periods which should be noted and understood. The Event Analysis (EA) program and the Compliance Monitoring and Enforcement Program (CMEP) activities can lengthen the standard data retention timeframes. For EA Category 3 events and higher, the regions can issue a data hold for the times around that event, and the data must be retained through the data hold period. While the entities involved in the event can always self-report possible non-compliance that occurred during the event, audit staff can also perform spot checks after the event concludes and/or examine the event on the next audit cycle. Thus, the standard retention window may have expired before the EA completes and/or the next audit occurs. Another exception to clarify is how to address the back-log in processing violations from NERC and the Regional Entity (RE) side.
2. We believe that registered entities are currently holding ALL evidence since 2007 because of the risk that an auditor can ask for any level of evidence regardless of retention time frames. Without a solid evidence retention policy approved by FERC, registered entities will continue their burdensome practices of keeping everything. As the Phase 2 Team notes, "evidence retention does not reduce risk or impact the reliability of the electric system". It is valuable to show compliance over a period of time; a corollary is that there is no increased reliability risk if an auditor does not look at evidence for some portion of an audit period. Currently, evidence review is predicated on the retention period stated in each standard, and an auditor can request evidence beyond the stated retention period if that period is shorter than the last audit. Instead, auditors should limit themselves to the evidence retention period and move on. We recommend that evidence retention should be the current record, e.g. for periodic tests, the most recent test results. We understand that auditors will not be able to see arbitrary recurring dates, but this should not matter. The intent is to verify that maintenance was accomplished (for example) within the specific period. Auditors should focus on issues that could impact future activities. This is a paradigm shift for our industry and we need to look forward and not into the past. This Concept greatly helps all entities by requiring limits on what past evidence auditors can review. In addition, if data collection is not helpful from a reliability perspective, it should not be performed in the first place. Reducing the amount of data collected would go a long way toward alleviating the burden of data retention.
3. The plethora of current evidence retention schemes has led to many companies defaulting to the worst case which burdens servers and the associated data management/backup policies. A handful of evidence retention schemes, clearly linked to the risk to the reliability of the Bulk Power System, should be sufficient. Although this may require modifications to current standards and a

possible revision to the NERC Rules of Procedure, this effort has significant value in making our compliance record preservations clear and meaningful.

4. We feel that this concept is not about retention of evidence but rather how much evidence should be kept for lower risk standards. We feel that it should be more specific in that the effort does not primarily concern itself with retention but rather having the "right size" of evidence to fit the risk of the requirements that are being monitored.
5. Data retention today is inconsistent and often subjective.
6. This concept will only be "worth the effort" if the ERO's compliance monitoring process recognizes and adheres to the data retention periods when conducting audits.
7. There should be more consistency with among standards in regards to evidence retention. For example, create an overall guideline that says recordings, logs, etc., of things that are done every day should always be a rolling 90 days or the last 90 days. Sometimes it's written differently among the various standards. Other evidence should be current year plus 1 previous year unless the entity has had a violation since its last audit; then it should be for the audit period. Then there is no guessing as to what needs to be kept.
8. There may be potential improvements in efficiency with this concept, but only if it reduces the need for the industry to routinely collect unnecessary data. We do not see a significant improvement in efficiency with only reducing the retention periods.
9. As the reliability risk decreases, the burden to retain detailed historical documentation should be relieved when possible. In addition, audit scope should respect the retention period. Small low-risk entity audit periods being extended out to nine years accentuates this need to restrict audit scope. Where increased risk is perceived by the Regional Entity, spot checks can be utilized to compensate for short retention periods.
10. Simplifying the evidence retention policy could potentially reduce costs, and shift focus away from administrative retention policies and more towards higher risk priorities.
11. As long as an entity must demonstrate compliance further back in time than the Data Retention for the requirement, it will not have a significant impact upon efficiency. This is because, unless there is another way of demonstrating compliance, entities will still need to keep the data past the Data Retention, as necessary, to demonstrate compliance in the time period (prior to the Data Retention). We suggest that the audit should only focus on the most current year for these types of requirements. Until this occurs, we will still need to keep all data based on inconsistencies between the data retention period and the audit period for each requirement (i.e. only keeping data for 1 year, yet for audit purposes; it must be necessary to access 3 years' worth of data).
12. Auditor demand for "alternate forms of compliance documentation" for time periods outside the retention requirement for the entire audit period should only occur in limited circumstances. It should be clearly understood that demonstration of compliance within the retention window demonstrates a culture of reliability. Should an entity pose a greater risk to the BES, spot checks can be implemented between scheduled audit periods. How the specific evaluation of data retention and evidence requirements for new technology needs to be detailed before the effort moves forward. Additionally, the current new technologies being considered for evaluation should be better detailed. One of the disadvantages listed is industry cost to implement. We agree that the there is an implementation cost, that cost is outweighed by the current cost of unneeded data retention and evidence requirements. Therefore, on a net basis, there is no cost disadvantage to the concept. The potential for the concept to require significant changes to the NERC Rules of Procedure (ROP) should be better detailed.
13. This SER team identified 45 evidence retention schemes, as well as inconsistency of application. Reducing the data retention schemes to less than ten (10) should provide industry with a consistent methodology and interpretation. Assigning data retention appropriate to risk factors will allow entities to focus their efforts on reliability of the BES and not on paperwork.

14. Many standards require retaining evidence since the last audit. However, for certain functions that can be 6 years or even longer based on the risk based approach to auditing. There should be a maximum duration for which data must be retained.
15. For this to be beneficial, it needs to be clear and consistent, both from one standard to the next, as well as universal application across the ERO. Currently, the shorter retention periods listed in the standards are of no benefit as evidence is generally retained indefinitely. In some cases, this adds a very minor compliance burden of providing evidence that evidence was retained for the specified period.
16. We recommend the evidence retention overhaul consider the two items outlined below. We support reviewing the referenced White Paper recommendations to determine if they are still appropriate, since it is nearly 5 years old, and suggest the CCC consider reconstituting the data retention team to reevaluate the findings and recommendations. This will allow any efforts on the initiative to be informed by updated information prior to moving forward with this activity. Finally, we suggest that the CCC may be a more appropriate committee to address evidence retention. Evidence retention is a key element of NERC's Compliance Monitoring and Enforcement Program (CMEP) and a Standard Drafting Team (SDT) may not have the required range of view to appropriately assess how to broadly address evidence retention. However, the mission of the CCC is "to engage with, support, and advise" NERC's CMEP.
17. Many Entities maintain all past evidence since there is a possibility of being asked of evidence from the past. With about 47 different evidence retention schemes it is easier to maintain all evidence. Even when there is a stated shorter retention period, there are statements such as: "… or 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" (within CIP-002-5.1a). Standards evidence is backward looking, and we agree that is used to assure past compliance but our Standards need to be forward looking.

Industry Comments NOT Supporting the Evidence Retention Concept

1. We note that regardless of a minimal data retention period (1 or 2 years), the RE has the authority to require compliance evidence up to and including the prior audit period.
2. We do not believe the work required to consider the vast amount of information and requirements surrounding evidence retention would result in value that exceeds the amount of work.
3. The evidence retention mechanisms are in place for specific reasons and have been tailored to audit cycles and the requirements themselves based on specific needs. We agree with the disadvantages identified. Although there may be some efficiency benefit it may not be commensurate with the burden of changes stakeholders and auditors would have to make to existing documentation.
4. We are unsure if this will result in a significant impact. Considering we have our own internal evidence retention policies, we will always err on the longest duration of retention. However, we do support a review and potential update of the referenced White Paper recommendations.
5. We do not believe that the effort will result in significant efficiency.

Analysis of Existing Evidence Retention Schemes

Introduction: Analysis of Existing Evidence Retention Schemes

Many Standards studied in 2014 are either inactive or were replaced with newer versions of the Standard. Therefore, the SER Phase 2 evidence retention team analyzed all mandatory and enforceable Operations and Planning (O&P) and Critical Infrastructure Protection (CIP) Standards focusing attention on the data retention requirements of each Standard and each requirement, which included the following Standards.

BAL	COM	CIP	EOP	FAC	INT	IRO
BAL-001-2	COM-001-3	CIP-002-5.1a	EOP-004-4	FAC-001-3	INT-004-3.1	IRO-001-4
BAL-002-3	COM-002-4	CIP-003-6	EOP-005-3	FAC-002-2	INT-006-4	IRO-002-5
BAL-003-1.1		CIP-004-6	EOP-006-3	FAC-003-4	INT-009-2.1	IRO-006-5
BAL-005-1		CIP-005-5	EOP-008-2	FAC-008-3	INT-010-2.1	IRO-008-2
		CIP-006-6	EOP-010-1	FAC-010-3		IRO-009-2
		CIP-007-6	EOP-011-1	FAC-011-3		IRO-010-2
		CIP-008-5		FAC-013-2		IRO-014-2
		CIP-009-6		FAC-014-2		IRO-017-1
		CIP-010-2				IRO-018-1(ii)
		CIP-011-2				
		CIP-014-2				

MOD	NUC	PER	PRC	TOP	TPL	VAR
MOD-001-1a	NUC-001-3	PER-003-1	PRC-001-	TOP-001-4	TPL-001-4	VAR-001-5
MOD-004-1		PER-004-2	1.1(ii)	TOP-002-4	TPL-007-1	VAR-002-4.1
MOD-008-1		PER-005-2	PRC-002-2	TOP-003-3		
MOD-020-0			PRC-004-5(i)	TOP-010-1(i)		
MOD-025-2			PRC-005-1.1b			
MOD-026-1			PRC-005-6			
MOD-027-1			PRC-006-3			
MOD-028-2			PRC-008-0			
MOD-029-2a			PRC-010-2			
MOD-030-3			PRC-011-0			
MOD-031-2			PRC-015-1			
MOD-032-1			PRC-016-1			
MOD-033-1			PRC-017-1			
			PRC-018-1			
			PRC-019-2			
			PRC-023-4			
			PRC-024-2			
			PRC-025-2			
			PRC-026-1			

Regional Standards were not included in the data analysis. Standards slated for retirement, but not yet formally retired were included in the analysis. The data analysis occurred on 6/14/2019. Since the date of that analysis some information may have changed.

Observations of Existing Evidence Retention Schemes

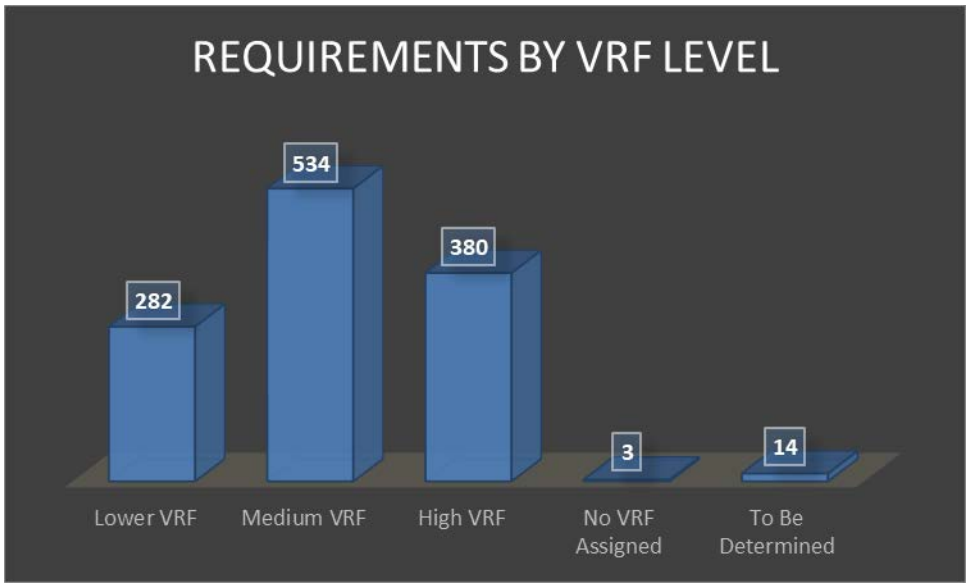
Number of Evidence Retention Schemes

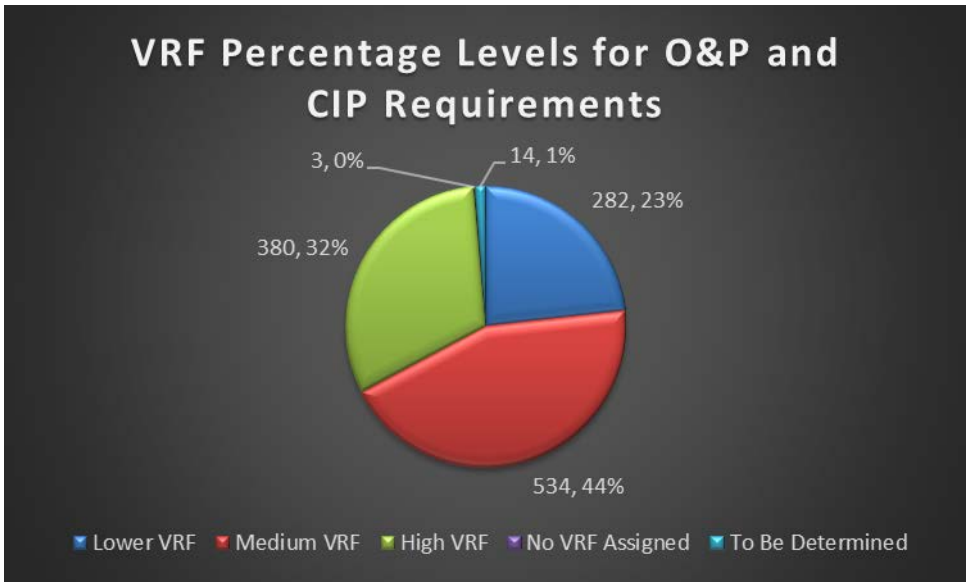
The Evidence Retention team discovered over 50 different evidence retention schemes throughout various Standards and requirements. Specific information on each scheme and applicable Standards and requirements is included in Appendix A.

VRF Analysis

- Approximately 1/3rd (32%) of the O&P and CIP Standards requirements have a High VRF level. These requirements have the highest violation risk factors and therefore evidence retention schemes for these requirements are important, and can have longer retention periods.

- The majority (44%) of the VRF risk levels for O&P and CIP Standard requirements are medium.
- Approximately 1/4th (23%) of the O&P and CIP Standards requirements have a Lower VRF level.
- O&P and CIP Standard requirements with "No VRF Assigned" or "To Be Determined" were statistically insignificant and had no impact on existing or proposed evidence retention schemes.





Applicability of Evidence Retention Schemes

Many current evidence retention schemes apply to only one requirement in one Standard (See Appendix A) for example, PRC-026-1, R3. The largest current evidence retention schemes include:

- "Last 3 Calendar Years" with over 40 applicable requirements.
- "Since Last Compliance Audit" with 34 applicable requirements.
- "Current plus 3 Previous Calendar Years" with 28 applicable requirements.

Similarity of Evidence Retention Schemes in Existing Standards

There was very little difference between certain evidence retention schemes, for example, the following retention schemes are described in Standard requirements and are basically the same (see Appendix A for detailed information by Standard and requirement):

- 12 Calendar Months vs. 12 Calendar Months Following Completion of each CAP
- 12 Calendar Months vs. One Calendar Year
- 12 Calendar Months vs. Current Year
- 12 Calendar Months vs. Last 12 Calendar Months
- Two Calendar Years vs. Current Calendar Year Plus One Previous Calendar Year

Plans, Assessments, Models, Tests and Documents Evidence Retention Schemes

There were many similarities when the current evidence retention schemes referred to plans, assessments, models, tests and documents. Many of the existing evidence retention schemes required the current document plus a previous version of the document, for example:

- Current and Previous Model Used to Determine Flowgates and TFC
- Current and Prior Transfer Capability Methodology Since Last Compliance Audit
- Current and Prior Versions
- Current Blackstart Testing Results and Previous Testing Results
- Current GMD Vulnerability Assessment and Preceding Assessment
- Current In-Force ATCID Provided by TSP and Prior Versions of ATCID
- Current In-Force Documents and Previous Documents

Poor Descriptions or Non-Existent Schemes

Some evidence retention schemes were poorly described, for example, “Current and Previous Calendar Years”, but the exact number of previous calendar years was not specified. Six requirements had no evidence retention schemes specified at all. One evidence retention scheme was extremely general and potentially no longer applicable, for example, “Retain Evidence of Any Path and Rating Prior to 1/1/94”, as shown in MOD-029-2a, R2.

Variations on a Theme

There were a lot of variations on the theme of “Current”, for example (see Appendix A):

- Current In-Force Data Specification for Analysis and Real-Time Monitoring
- Current In-Force Documents
- Current In-Force Documents and Previous Documents
- Current In-Force Facility Ratings Methodology
- Current In-Force Outage Coordination Process
- Current Model Used to Calculate TTC
- Current Planning Analysis Results
- Current Plus 1 Previous Calendar Year
- Current Plus 2 Previous Calendar Years
- Current Plus 3 Previous Calendar Years
- Current Version and Prior Version of The TTC Study Reports
- Current Year

Evidence Retention Language

NERC Reliability Standards contain language in the data retention or evidence retention sections that are often exactly the same from Standard to Standard as noted below. Sometimes, however, the language

differs slightly, which makes the evidence retention process complicated and confusing for both registered entities and compliance enforcement authorities (CEA). Here are some examples of potentially confusing evidence retention language in existing mandatory Standards:

- 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 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.
- In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.
- If a Transmission Service Provider or Transmission Operator is found noncompliant, it shall keep information related to the non-compliance until found compliant.
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.
- If a Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider 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.
- If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.
- Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor.
- The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.
- Not all NERC Standards have a “Data Retention” section.
- Some Standards have a single data retention directive.
- Some Standards have data retention specifications for each requirement in the Standard.
- Some Standards have data retention specifications related to the Standard’s measurements.

Evidence Categories

The existing NERC Standards describe Data and Evidence retention periods that attempt to address evidence that falls into one or more of the following evidence categories:

1. Voice Data
2. Logs
3. Documents, Processes and Plans
4. Models and Methodologies
5. Assessments, Lists, Records and Studies
6. Agreements

Different Headings in NERC Standards

The team discovered that two headings were used interchangeably in the NERC Standards without any direction as to which one is preferred:

1. Data Retention
2. Evidence Retention

General Observations

The Evidence Retention team observed:

- The data/evidence retention schemes were somewhat arbitrary and without apparent rationale.
- Some evidence retention schemes were excessively long, some very short, but there was no consistent rationale for retention length.
- Similar evidence categories described in different Standards have different evidence retention schemes.
- Evidence retention schemes vary within specific Standards by requirement.
- Some evidence retention schemes are one-of-a-kind, that is, they appear only once. This is usually because they are so specific they apply only to one Standard and one requirement. These overly specific data retention schemes are not necessary, for example PRC-026-1, R3.
- The higher the risk the longer records should be kept. The lower the risk the shorter records should be kept.

Analysis of Requirement Text, Measures, and Evidence Retention

The Role of Measures vs. Evidence Retention

In its pure form, the Measures section of NERC Standards indicates what evidence must be collected. The Evidence Retention section indicates how long to keep the specified evidence. However, this gets complicated and confusing when the measures section of the Standard indicates how long to keep the evidence. There is no direction to Standard Drafting Teams (SDT) on what specific information should be included in a measure and what should be included in the evidence retention sections.

Rules of Procedure and Measures

The ROP speaks about measures using general guidance language:

> **Measurability — Each performance Requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that Requirement. Each performance Requirement shall have one or more associated measures used to objectively evaluate compliance with the Requirement. If performance can be practically measured quantitatively, metrics shall be provided to determine satisfactory performance.[10]**
>
> **Measure: Provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.[11]**

The ROP does not specifically speak to evidence retention schemes as related to measures. This is left to the discretion of SDTs.

Observations Regarding Measures and Evidence Retention

The evidence retention team analyzed measures and evidence retention for high VRF requirements and observed the following:

- Sometimes measures clearly indicate what evidence should be collected to demonstrate compliance with no reference to how long to retain the evidence.
- In some instances, the measures indicate not only what evidence to collect, but how long to retain evidence. This creates confusion between what's listed in the measures and what's listed in the evidence retention section of the Standard.

[10] NERC ROP, Section 302, pg. 4. NERC ROP, Effective 7/19/18
[11] Ibid, Section 2.0: Elements of a Reliability Standard, Subsection 2.5: Elements of a Reliability Standard, pg. 8.

- Some Standards have statements in them that give CEAs authority to ask an entity to provide evidence that it was compliance for the full-time period since the last audit even if the evidence retention section of the Standard indicates a much shorter retention period. This causes entities to save data for much longer periods just in case they are asked for it. Evidence retention schemes should be clear for both CEAs and registered entities and data should not be stored beyond defined limits.
- There appears to be some uncertainty among different SDTs regarding the purpose and differences between measures and the data retention portions of a Standard.

Evidence Retention Recommendations

Recommended Evidence Retention Schemes

The evidence retention team simplified the existing evidence retention schemes to a set of five evidence retention schemes to cover all NERC O&P and CIP Standards and requirements as shown in the following table.

Recommended Data/Evidence Retention Schemes	Rationale for the Data/Evidence Retention Scheme
1. Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review. If revised within the last year, the prior version should also be retained.	This satisfies the need for auditors to see the most recent documentation in a variety of areas. What is most important is the current document and that document should have a revision history showing that it is regularly reviewed and updated. In some instances, evidence retention may exceed a three year period.
2. Most recent full testing records with evidence of previous testing intervals.	This satisfies the requirements to complete and document various tests and includes the requirement to have evidence of the previous full testing records. In some instances, evidence retention may exceed a three year period.
3. Rolling 3 Months data retention period.	Data retention schemes that require significant computer storage, such as voice and audio recordings, could be reduced to 3 months of rolling history.
4. Rolling 12 Months data retention period.	This satisfies existing evidence retention scheme requirements to have at least 12 months of data. Based the type of data or reliability risk, it may not be necessary to retain 36 months of data.
5. Rolling 36 Months data retention period.	Many existing evidence retention schemes call for a three year (36 month) retention schedule. The 36 month data retention is retained with the addition of "rolling".

Additional Recommendations

The SER Phase 2 team Data/Evidence Retention Project team recommends the following:

1. Pursue Rules of Procedure changes for evidence retention to minimize administrative burden. (NERC Staff)
2. Retire Compliance Bulletin #2011-001 Data Retention Requirements, once ROP changes are in effect or publish CMEP guidance to supersede the bulletin. (NERC Staff and CCC)
3. Concurrent with ROP changes, update Standard Drafting Teams (SDTs) references and notify active SDTs, with the minimum options for risk-based data retention schemes, as described above. In addition, the headings within Reliability Standard should be consistently named "Data and Evidence Retention Period". (SC)

4. If desired, concurrent with ROP changes, establish a project to revise evidence retention schemes for enforceable Reliability Standards with a Standard Drafting Team, Periodic Review team, or other mechanism. (SC and NERC Staff)
5. Ensure changes to CMEP evidence retention processes are made in associated documents and communicated with ERO Enterprise staff, such as NERC Auditor's Manual, training materials, etc. (NERC Staff)
6. Ensure final recommendations of SER Evidence Retention are circulated with the CCC, SC, and NERC staff, and recommendations are incorporated into respective work plans in 2020. (CCC, SC, NERC Staff)

Appendix A – Results of Analyzing Current Evidence Retention Schemes

List of Existing Evidence Retention Schemes in NERC Standards

The following table summarizes an analysis of data/evidence retention schemes listed in active NERC O&P and CIP Standards. NOTE: The list did not exclude Standards and requirements slated for retirement as part of SER Phase 1 efforts since, at the time of this report, retirements were not yet effective.

Current Evidence Retention Scheme	Total	Standards and Requirements List
1. 12 Calendar Months Following Completion of each CAP	1	PRC-026-1, R3
2. 90 Calendar Days	3	CIP-007-6, R4 IRO-018-1(i), R3 PRC-001-1.1(ii), R3
3. 90 Calendar Days Voice, 12 Months for Logs	2	FAC-003-4, R4 TOP-002-4, R1
4. Approved Plan and Previous Plan Since Last Compliance Audit	2	EOP-005-3, R1 EOP-006-3, R1
5. Current and Previous Calendar Years (time not specified)	1	EOP-008-2, R7
6. Current and Previous Model Used to Determine Flowgates and TFC	1	MOD-030-3, R2
7. Current and Previous Planning Assessment	1	TPL-001-4, R1
8. Current and Prior Transfer Capability Methodology Since Last Compliance Audit	1	FAC-013-2, R1
9. Current and Prior Versions	1	EOP-005-3, R6
10. Current Blackstart Testing Results and Previous Testing Results	1	EOP-005-3, R7
11. Current Calendar Year Plus One Previous Calendar Year, except operator logs and voice recordings - retain for 90 calendar days	7	COM-002-4, R1, R2 IRO-018-1(i), R1 TOP-001-4, R1, R15, R22 TOP-010-1(i), R1
12. Current GMD Vulnerability Assessment and Preceding Assessment	1	TPL-007-1, R4
13. Current In-Force Agreement	1	NUC-001-3, R2
14. Current In-Force ATCID Provided by TSP and Prior Versions of ATCID Since Last Compliance Audit	3	MOD-001-1a, R3 MOD-029-2a, R1 MOD-030-3, R1
15. Current In-Force Data Specification for Analysis and Real-Time Monitoring	1	TOP-003-3, R2
16. Current In-Force Documents	1	PRC-001-1.1(II), R1
17. Current In-Force Documents and Previous Documents Since Last Compliance Audit	3	EOP-008-2, R8 IRO-002-5, R1 IRO-014-3, R1
18. Current In-Force Facility Ratings Methodology Since Last Compliance Audit	2	FAC-008-3, R2, R3
19. Current In-Force Outage Coordination Process Since Last Compliance Audit	1	IRO-017-1, R1
20. Current Model Used to Calculate TTC	2	MOD-028-2, R2 MOD-029-2a, R1

Current Evidence Retention Scheme	Total	Standards and Requirements List
21. Current OPA, Real-time Monitoring, and Real-time Assessments Since Last Audit	2	IRO-010-2, R1 TOP-003-3, R1
22. Current Operating Plan and Previous Plans Since Last Compliance Audit	5	EOP-004-4, R1 EOP-008-2, R1, R6 EOP-011-1, R1, R2
23. Current Planning Analysis Results	1	NUC-001-3, R3
24. Current Plus 1 Previous Calendar Year	7	IRO-002-5, R5 MOD-001-1a, R2, R6 MOD-030-3, R5 TOP-001-4, R20, R23 VAR-002-4.1, R1
25. Current Plus 2 Previous Calendar Years	4	NUC-001-3, R4, R5 PER-004-2, R1 PRC-001-1.1(ii), R3
26. Current Plus 3 Previous Calendar Years	28	BAL-001-2, R1 BAL-002-3, R2 BAL-003-1.1, R1 BAL-005-1, R1 EOP-005-3, R2, R3, R4, R5 EOP-006-3, R2, R3, R4, R5, R6 FAC-008-3, R1 IRO-014-3, R6 MOD-001-1a, R5 MOD-004-1, R1, R2, R3, R4, R6, R10, R11 MOD-008-1, R2, R4 MOD-029-2a, R3, R7 MOD-030-3, R2.2.
27. Current Version and Prior Version of The TTC Study Reports	1	MOD-029-2a, R2
28. Current Year	1	EOP-008-2, R2
29. Five Calendar Years	4	PRC-002-2, R1, R5 TPL-007-1, R1, R7
30. Last 12 Calendar Months	13	FAC-014-2, R1 IRO-014-3, R5 MOD-028-2, R3, R4, R10 MOD-030-3, R2.1, R4 PRC-004-5(i), R1, R5, R6 PRC-006-3, R6 PRC-026-1, R2 VAR-001-5, R1
31. Last 12 Calendar Months Plus Current Month	3	IRO-006-5, R1 IRO-006-East-2, R1, R2
32. Last 14 Days, Past 30 Days Daily Values, And Past 60 Days for Monthly Values	3	MOD-028-2, R8 MOD-029-2a, R5 MOD-030-3, R6
33. Last 3 Calendar Years	Over 40	CIP-002-5.1a, All CIP-003-6, All CIP-004-6, All CIP-005-5, All CIP-006-6, All CIP-007-6, All CIP-008-5, All CIP-009-6, All CIP-010-2, All CIP-011-2, All CIP-014-2, All EOP-010-1, R1 FAC-001-3, R1 FAC-002-2, R1 FAC-003-4, R1, R2, R3, R5, R6, R7

Current Evidence Retention Scheme	Total	Standards and Requirements List
		FAC-008-3, R4, R7, R8 IRO-010-2, R2 IRO-017-1, R2, R3, R4 MOD-026-1, R1, R3 MOD-027-1, R1, R3 PRC-006-NPCC-1, R1 PRC-018-1, R1 PRC-023-4, R1 PRC-024-2, R1 PRC-025-2, R1 TOP-003-3, R3, R4
34. Last Load Control or Active Power/Frequency Control System Model Verification	1	MOD-027-1, R2
35. Latest Excitation Control System or Plant volt/var Control Function Model	1	MOD-026-1, R2
36. Latest Transmittals and Receipts	1	NUC-001-3, R1
37. Most Recent 12 Calendar Months Except Operator Logs and Voice Recordings - Retain for 90 Calendar Days	3	IRO-002-5, R3 TOP-001-4, R21, R24
38. Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	7	COM-001-3, R1, R12, R13, R3, R5, R7, R8
39. Most Recent 3 Calendar Months Plus Current Month	6	INT-004-3.1, R1, R3 INT-006-4, R1, R2 INT-009-2.1, R1 INT-010-2.1, R1
40. Most Recent 90 Calendar Days	2	IRO-010-2, R3 TOP-003-3, R5
41. Most Recent 90-Calendar Days Voice, Most Recent 12 Calendar Months Documentation	2	IRO-001-4, R1, R2
42. Most Recent List of Circuits	1	PRC-023-4, R6
43. None Specified	6	MOD-020-0, R1 PRC-008-0, R1 PRC-011-0, R1 PRC-015-1, R1 PRC-016-1, R1 PRC-017-1, R1
44. One Calendar Year	1	PRC-026-1, R1
45. One Year from SOL Methodology Change	2	FAC-010-3, R1 FAC-011-3, R1
46. Retain Evidence of Any Path and Rating Prior to 1/1/94	1	MOD-029-2a, R2
47. Rolling 12-Month Period	1	IRO-009-2, R1
48. Rolling 30-Days	4	IRO-008-2, R4 IRO-018-1(ii), R2 TOP-001-4, R13 TOP-010-1(i), R3
49. Rolling 90-Calendar Days for Voice, 12 Months for Operating Logs	3	IRO-008-2, R1 IRO-014-3, R3 TOP-002-4, R1
50. Since Last Compliance Audit	34	BAL-002-3, R1 EOP-004-4, R2 EOP-008-2, R3, R4, R5 EOP-011, R3, R5, R6 FAC-008-3, R1 FAC-013-2, R2 MOD-001-1a, R1 MOD-008-1, R1 MOD-025-2, R1, R3 MOD-028-2, R1

Current Evidence Retention Scheme	Total	Standards and Requirements List
		MOD-031-2, R1 MOD-032-1, R1 MOD-033-1, R1 PER-005-3, R1, R2 PRC-005-6, R1, R2, R5 PRC-006-3, R1, R10, R7, R8, R9 TPL-001-4, R2, R3, R4, R5, R6, R7
51. Since Last Compliance Audit Plus one Previous Compliance Audit	2	EOP-005-3, R10 EOP-006-3, R8
52. Six Calendar Years	3	PRC-006-3, R11 PRC-010-2, R1 PRC-019-2, R1
53. Three Calendar Years	6	PRC-002-2, R2, R6, R7 PRC-005-1.1b, R1 TOP-001-4, R12, R14
54. Three Years or Since Last Compliance Audit Whichever is Longer	1	PER-003-1, R1

Appendix B: VRF File Listings

This appendix contains the VRF designations for the CIP and O&P Standards.

High VRF List

For simplicity sake, the data from the NERC VRF Matrix was sorted on whole requirement numbers, for example, R1., R2., R3., etc. Sub-requirement numbers, for example, R1.1., R1.1.1. etc. were not included in the data analysis, because by default sub-requirements inherit the parent VRF level.

Standard	Req.	VRF
BAL-002-3	R1.	HIGH
BAL-002-3	R2.	HIGH
BAL-003-1.1	R1.	HIGH
CIP-002-5.1a	R1.	HIGH
CIP-014-2	R1.	HIGH
COM-001-3	R1.	HIGH
COM-001-3	R2.	HIGH
COM-001-3	R3.	HIGH
COM-001-3	R4.	HIGH
COM-001-3	R5.	HIGH
COM-001-3	R6.	HIGH
COM-001-3	R8.	HIGH
COM-001-3	R12.	HIGH
COM-002-4	R5.	HIGH
COM-002-4	R6.	HIGH
COM-002-4	R7.	HIGH
EOP-005-3	R1.	HIGH
EOP-006-3	R1.	HIGH
EOP-008-2	R3.	HIGH
EOP-008-2	R4.	HIGH
EOP-011-1	R1.	HIGH
EOP-011-1	R2.	HIGH
EOP-011-1	R3.	HIGH
EOP-011-1	R4.	HIGH
EOP-011-1	R5.	HIGH
EOP-011-1	R6.	HIGH
FAC-003-4	R1.	HIGH
FAC-003-4	R2.	HIGH
FAC-014-2	R5.	HIGH
IRO-001-4	R1.	HIGH
IRO-001-4	R2.	HIGH
IRO-001-4	R3.	HIGH
IRO-002-5	R2.	HIGH
IRO-002-5	R4.	HIGH
IRO-002-5	R5.	HIGH
IRO-002-5	R6.	HIGH
IRO-006-5	R1.	HIGH
IRO-008-2	R4.	HIGH
IRO-008-2	R5.	HIGH
IRO-009-2	R2.	HIGH
IRO-009-2	R3.	HIGH
IRO-009-2	R4.	HIGH
IRO-014-3	R4.	HIGH
IRO-014-3	R5.	HIGH
IRO-014-3	R6.	HIGH
IRO-014-3	R7.	HIGH
IRO-018-1(i)	R1.	HIGH
NUC-001-3	R4.	HIGH
NUC-001-3	R5.	HIGH
NUC-001-3	R7.	HIGH
NUC-001-3	R8.	HIGH
PER-003-1	R1.	HIGH
PER-003-1	R2.	HIGH
PER-003-1	R3.	HIGH
PER-004-2	R1.	HIGH
PER-004-2	R2.	HIGH
PER-005-2	R3.	HIGH
PRC-001-1.1(ii)	R1.	HIGH
PRC-001-1.1(ii)	R4.	HIGH
PRC-001-1.1(ii)	R5.	HIGH
PRC-004-5(i)	R1.	HIGH
PRC-004-5(i)	R2.	HIGH
PRC-004-5(i)	R3.	HIGH
PRC-004-5(i)	R4.	HIGH
PRC-004-5(i)	R5.	HIGH
PRC-004-5(i)	R6.	HIGH
PRC-005-1.1b	R1.	HIGH
PRC-005-6	R3.	HIGH
PRC-005-6	R4.	HIGH
PRC-006-3	R3.	HIGH
PRC-006-3	R4.	HIGH
PRC-006-3	R5.	HIGH
PRC-006-3	R9.	HIGH
PRC-006-3	R10.	HIGH
PRC-006-3	R15.	HIGH
PRC-010-2	R1.	HIGH
PRC-010-2	R2.	HIGH
PRC-017-1	R1.	HIGH
PRC-023-4	R1.	HIGH
PRC-023-4	R2.	HIGH
PRC-023-4	R6.	HIGH
PRC-025-2	R1.	HIGH
PRC-026-1	R2.	HIGH
TOP-001-4	R1.	HIGH
TOP-001-4	R2.	HIGH
TOP-001-4	R3.	HIGH
TOP-001-4	R4.	HIGH
TOP-001-4	R5.	HIGH
TOP-001-4	R6.	HIGH
TOP-001-4	R7.	HIGH
TOP-001-4	R8.	HIGH
TOP-001-4	R10.	HIGH
TOP-001-4	R11.	HIGH
TOP-001-4	R12.	HIGH
TOP-001-4	R13.	HIGH
TOP-001-4	R14.	HIGH
TOP-001-4	R16.	HIGH
TOP-001-4	R17.	HIGH
TOP-001-4	R18.	HIGH
TOP-001-4	R20.	HIGH
TOP-001-4	R23.	HIGH
TOP-010-1(i)	R1.	HIGH
TOP-010-1(i)	R2.	HIGH
TPL-001-4	R1.	HIGH
TPL-001-4	R2.	HIGH
TPL-007-1	R2.	HIGH
TPL-007-1	R4.	HIGH
TPL-007-1	R7.	HIGH
VAR-001-5	R1.	HIGH
VAR-001-5	R2.	HIGH
VAR-001-5	R3.	HIGH

Medium VRF

Standard	Req.	VRF
BAL-001-2	R1.	Medium
BAL-001-2	R2.	Medium
BAL-002-3	R3.	Medium
BAL-003-1.1	R2.	Medium
BAL-003-1.1	R3.	Medium
BAL-003-1.1	R4.	Medium
BAL-005-1	R1.	Medium
BAL-005-1	R2.	Medium
BAL-005-1	R3.	Medium

Standard	Req.	VRF
BAL-005-1	R4.	Medium
BAL-005-1	R5.	Medium
BAL-005-1	R6.	Medium
BAL-005-1	R7.	Medium
CIP-003-6	R1.	Medium
CIP-003-6	R3.	Medium
CIP-004-6	R3.	Medium
CIP-004-6	R4.	Medium
CIP-004-6	R5.	Medium
CIP-005-5	R1.	Medium
CIP-005-5	R2.	Medium
CIP-006-6	R1.	Medium
CIP-006-6	R2.	Medium
CIP-006-6	R3.	Medium
CIP-007-6	R1.	Medium
CIP-007-6	R2.	Medium
CIP-007-6	R3.	Medium
CIP-007-6	R4.	Medium
CIP-007-6	R5.	Medium
CIP-009-6	R1.	Medium
CIP-010-2	R1.	Medium
CIP-010-2	R2.	Medium
CIP-010-2	R3.	Medium
CIP-010-2	R4.	Medium
CIP-011-2	R1.	Medium
CIP-014-2	R2.	Medium
COM-001-3	R7.	Medium
COM-001-3	R9.	Medium
COM-001-3	R10.	Medium
COM-001-3	R11.	Medium
COM-001-3	R13.	Medium
COM-002-4	R4.	Medium
EOP-004-4	R2.	Medium
EOP-005-3	R2.	Medium
EOP-005-3	R3.	Medium
EOP-005-3	R4.	Medium
EOP-005-3	R6.	Medium
EOP-005-3	R7.	Medium
EOP-005-3	R8.	Medium
EOP-005-3	R9.	Medium
EOP-005-3	R10.	Medium
EOP-005-3	R11.	Medium
EOP-005-3	R12.	Medium
EOP-005-3	R13.	Medium
EOP-005-3	R14.	Medium
EOP-005-3	R15.	Medium
EOP-005-3	R16.	Medium
EOP-006-3	R3.	Medium
EOP-006-3	R4.	Medium
EOP-006-3	R5.	Medium
EOP-006-3	R7.	Medium
EOP-006-3	R8.	Medium
EOP-008-2	R1.	Medium
EOP-008-2	R5.	Medium
EOP-008-2	R6.	Medium
EOP-008-2	R7.	Medium
EOP-008-2	R8.	Medium
EOP-010-1	R1.	Medium

Standard	Req.	VRF
EOP-010-1	R2.	Medium
EOP-010-1	R3.	Medium
FAC-002-2	R1.	Medium
FAC-002-2	R2.	Medium
FAC-002-2	R3.	Medium
FAC-002-2	R4.	Medium
FAC-002-2	R5.	Medium
FAC-003-4	R4.	Medium
FAC-003-4	R5.	Medium
FAC-003-4	R6.	Medium
FAC-003-4	R7.	Medium
FAC-008-3	R2.	Medium
FAC-008-3	R3.	Medium
FAC-008-3	R6.	Medium
FAC-008-3	R7.	Medium
FAC-008-3	R8.	Medium
FAC-011-3	R3.	Medium
FAC-013-2	R1.	Medium
FAC-013-2	R4.	Medium
FAC-014-2	R1.	Medium
FAC-014-2	R2.	Medium
FAC-014-2	R3.	Medium
FAC-014-2	R4.	Medium
FAC-014-2	R6.	Medium
INT-009-2.1	R1.	Medium
INT-009-2.1	R2.	Medium
INT-009-2.1	R3.	Medium
IRO-002-5	R1.	Medium
IRO-002-5	R3.	Medium
IRO-008-2	R1.	Medium
IRO-008-2	R2.	Medium
IRO-008-2	R3.	Medium
IRO-008-2	R6.	Medium
IRO-009-2	R1.	Medium
IRO-014-3	R1.	Medium
IRO-014-3	R3.	Medium
IRO-017-1	R1.	Medium
IRO-017-1	R2.	Medium
IRO-017-1	R3.	Medium
IRO-017-1	R4.	Medium
IRO-018-1(i)	R2.	Medium
IRO-018-1(i)	R3.	Medium
MOD-001-1a	R1.	Medium
MOD-001-1a	R2.	Medium
MOD-001-1a	R3.	Medium
MOD-001-1a	R6.	Medium
MOD-001-1a	R7.	Medium
MOD-001-1a	R8.	Medium
MOD-001-1a	R9.	Medium
MOD-004-1	R1.	Medium
MOD-004-1	R2.	Medium
MOD-004-1	R3.	Medium
MOD-004-1	R4.	Medium
MOD-004-1	R5.	Medium
MOD-004-1	R6.	Medium
MOD-004-1	R7.	Medium
MOD-004-1	R8.	Medium
MOD-004-1	R11.	Medium

Standard	Req.	VRF
MOD-004-1	R12.	Medium
MOD-008-1	R1.	Medium
MOD-008-1	R2.	Medium
MOD-008-1	R4.	Medium
MOD-008-1	R5.	Medium
MOD-025-2	R1.	Medium
MOD-025-2	R2.	Medium
MOD-025-2	R3.	Medium
MOD-026-1	R2.	Medium
MOD-026-1	R6.	Medium
MOD-027-1	R2.	Medium
MOD-027-1	R5.	Medium
MOD-031-2	R1.	Medium
MOD-031-2	R2.	Medium
MOD-031-2	R3.	Medium
MOD-031-2	R4.	Medium
MOD-032-1	R2.	Medium
MOD-032-1	R4.	Medium
MOD-033-1	R1.	Medium
NUC-001-3	R1.	Medium
NUC-001-3	R2.	Medium
NUC-001-3	R3.	Medium
NUC-001-3	R6.	Medium
NUC-001-3	R9.	Medium
PER-005-2	R1.	Medium
PER-005-2	R2.	Medium
PER-005-2	R4.	Medium
PER-005-2	R5.	Medium
PER-005-2	R6.	Medium
PRC-005-6	R1.	Medium
PRC-005-6	R2.	Medium
PRC-005-6	R5.	Medium
PRC-006-3	R1.	Medium
PRC-006-3	R2.	Medium
PRC-006-3	R11.	Medium
PRC-006-3	R12.	Medium
PRC-006-3	R13.	Medium
PRC-008-0	R1.	Medium
PRC-008-0	R2.	Medium
PRC-010-2	R3.	Medium
PRC-010-2	R4.	Medium
PRC-010-2	R5.	Medium
PRC-011-0	R1.	Medium
PRC-015-1	R1.	Medium
PRC-015-1	R2.	Medium
PRC-016-1	R1.	Medium
PRC-016-1	R2.	Medium
PRC-019-2	R1.	Medium
PRC-019-2	R2.	Medium
PRC-023-4	R3.	Medium
PRC-024-2	R1.	Medium
PRC-024-2	R2.	Medium
PRC-026-1	R1.	Medium
PRC-026-1	R3.	Medium
PRC-026-1	R4.	Medium
TOP-001-4	R9.	Medium
TOP-001-4	R15.	Medium
TOP-001-4	R19.	Medium

Standard	Req.	VRF
TOP-001-4	R21.	Medium
TOP-001-4	R22.	Medium
TOP-001-4	R24.	Medium
TOP-002-4	R1.	Medium
TOP-002-4	R2.	Medium
TOP-002-4	R3.	Medium
TOP-002-4	R4.	Medium
TOP-002-4	R5.	Medium
TOP-002-4	R6.	Medium
TOP-002-4	R7.	Medium
TOP-003-3	R5.	Medium
TOP-010-1(i)	R3.	Medium
TOP-010-1(i)	R4.	Medium
TPL-001-4	R3.	Medium
TPL-001-4	R4.	Medium
TPL-001-4	R5.	Medium
TPL-001-4	R6.	Medium
TPL-001-4	R8.	Medium
TPL-007-1	R3.	Medium
TPL-007-1	R5.	Medium
TPL-007-1	R6.	Medium
VAR-001-5	R5.	Medium
VAR-002-4.1	R1.	Medium
VAR-002-4.1	R2.	Medium
VAR-002-4.1	R3.	Medium
VAR-002-4.1	R4.	Medium

Lower VRF List

Standard Number	Req.	VRF
CIP-002-5.1a	R2.	LOWER
CIP-003-6	R2.	LOWER
CIP-003-6	R4.	LOWER
CIP-004-6	R1.	LOWER
CIP-004-6	R2.	LOWER
CIP-008-5	R1.	LOWER
CIP-008-5	R2.	LOWER
CIP-008-5	R3.	LOWER
CIP-009-6	R2.	LOWER
CIP-009-6	R3.	LOWER
CIP-011-2	R2.	LOWER
COM-002-4	R1.	LOWER
COM-002-4	R2.	LOWER
COM-002-4	R3.	LOWER
EOP-004-4	R1.	LOWER
EOP-005-3	R5.	LOWER
EOP-006-3	R2.	LOWER
EOP-006-3	R6.	LOWER
EOP-008-2	R2.	LOWER
FAC-001-3	R1.	LOWER
FAC-001-3	R2.	LOWER
FAC-001-3	R3.	LOWER
FAC-001-3	R4.	LOWER
FAC-003-4	R3.	LOWER
FAC-008-3	R1.	LOWER
FAC-008-3	R4.	LOWER
FAC-008-3	R5.	LOWER
FAC-010-3	R1.	LOWER
FAC-010-3	R3.	LOWER
FAC-010-3	R4.	LOWER
FAC-010-3	R5.	LOWER
FAC-011-3	R1.	LOWER
FAC-011-3	R4.	LOWER
FAC-013-2	R2.	LOWER
FAC-013-2	R3.	LOWER
FAC-013-2	R5.	LOWER
FAC-013-2	R6.	LOWER
INT-004-3.1	R1.	LOWER
INT-004-3.1	R2.	LOWER
INT-004-3.1	R3.	LOWER
INT-006-4	R1.	LOWER
INT-006-4	R2.	LOWER
INT-006-4	R3.	LOWER
INT-006-4	R4.	LOWER
INT-006-4	R5.	LOWER
INT-010-2.1	R1.	LOWER
INT-010-2.1	R2.	LOWER
INT-010-2.1	R3.	LOWER
IRO-010-2	R1.	LOWER
IRO-010-2	R2.	LOWER
IRO-010-2	R3.	LOWER
IRO-014-3	R2.	LOWER
MOD-001-1a	R4.	LOWER
MOD-001-1a	R5.	LOWER
MOD-004-1	R9.	LOWER
MOD-004-1	R10.	LOWER
MOD-008-1	R3.	LOWER
MOD-020-0	R1.	LOWER
MOD-026-1	R1.	LOWER
MOD-026-1	R3.	LOWER
MOD-026-1	R4.	LOWER
MOD-026-1	R5.	LOWER
MOD-027-1	R1.	LOWER
MOD-027-1	R3.	LOWER
MOD-027-1	R4.	LOWER
MOD-028-2	R1.	LOWER
MOD-028-2	R2.	LOWER
MOD-028-2	R3.	LOWER
MOD-028-2	R4.	LOWER
MOD-028-2	R5.	LOWER
MOD-028-2	R6.	LOWER
MOD-028-2	R7.	LOWER
MOD-028-2	R8.	LOWER
MOD-028-2	R9.	LOWER
MOD-028-2	R10.	LOWER
MOD-028-2	R11.	LOWER
MOD-029-2a	R1.	LOWER
MOD-029-2a	R2.	LOWER
MOD-029-2a	R3.	LOWER
MOD-029-2a	R4.	LOWER
MOD-029-2a	R5.	LOWER
MOD-029-2a	R6.	LOWER
MOD-029-2a	R7.	LOWER
MOD-029-2a	R8.	LOWER
MOD-032-1	R1.	LOWER
MOD-032-1	R3.	LOWER

MOD-033-1	R2.	LOWER
PRC-002-2	R1.	LOWER
PRC-002-2	R2.	LOWER
PRC-002-2	R3.	LOWER
PRC-002-2	R4.	LOWER
PRC-002-2	R5.	LOWER
PRC-002-2	R6.	LOWER
PRC-002-2	R7.	LOWER
PRC-002-2	R8.	LOWER
PRC-002-2	R9.	LOWER
PRC-002-2	R10.	LOWER
PRC-002-2	R11.	LOWER
PRC-002-2	R12.	LOWER
PRC-005-1.1b	R2.	LOWER
PRC-006-3	R6.	LOWER
PRC-006-3	R7.	LOWER
PRC-006-3	R8.	LOWER
PRC-006-3	R14.	LOWER
PRC-010-2	R6.	LOWER
PRC-010-2	R7.	LOWER
PRC-010-2	R8.	LOWER
PRC-011-0	R2.	LOWER
PRC-015-1	R3.	LOWER
PRC-016-1	R3.	LOWER
PRC-017-1	R2.	LOWER
PRC-018-1	R1.	LOWER
PRC-018-1	R2.	LOWER
PRC-018-1	R3.	LOWER
PRC-018-1	R4.	LOWER

Appendix C: Recommended Evidence Retention for High VRF Requirements

The following table is a compilation of all High VRF NERC Standard requirements for O&P and CIP Standards as of 6/14/2019. It provides a summary of the current evidence retention scheme and the recommended evidence retention scheme. Medium and lower VRF requirements were also considered, but the Evidence Retention team decided to focus on the highest risks to the BES as indicated in the Evidence Retention project objectives. Medium and lower VRF requirements would be subject to the same set of recommended evidence retention schemes.

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
BAL-002-3	R1.	Since Last Compliance Audit	Rolling 12 months data retention period.
BAL-002-3	R2.	Current Plus 3 Previous Calendar Years	Rolling 36 months data retention period.
BAL-003-1.1	R1.	Current Plus 3 Previous Calendar Years	Rolling 36 months data retention period.
CIP-002-5.1a	R1.	Last 3 Calendar Years	Rolling 36 months data retention period.
CIP-014-2	R1.	Last 3 Calendar Years	Rolling 36 months data retention period.
COM-001-3	R1.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.[12]
COM-001-3	R2.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-001-3	R12.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-001-3	R3.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-001-3	R4.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-001-3	R5.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-001-3	R6.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.

[12] Except voice recordings where the retention period would be 3 rolling months as found in certain requirements (COM-001-3, COM-002-4, IRO-002-5, IRO-018-1, TOP-001-4, and TOP-010-1(i)).

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
COM-001-3	R8.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-002-4	R5.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-002-4	R6.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
COM-002-4	R7.	Most Recent 12 Calendar Months Except Voice Recordings, Most Recent 90 Calendar Days	Rolling 12 months data retention period.
EOP-005-3	R1.	Approved Plan and Previous Plan Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-006-3	R1.	Approved Plan and Previous Plan Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-008-2	R3.	Since Last Compliance Audit	Rolling 36 months data retention period.
EOP-008-2	R4.	Since Last Compliance Audit	Rolling 36 months data retention period.
EOP-011-1	R1.	Current Operating Plan and Previous Plans Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-011-1	R2.	Current Operating Plan and Previous Plans Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-011-1	R3.	Since Last Compliance Audit	Rolling 36 months data retention period.
EOP-011-1	R4.	Since Last Compliance Audit	Rolling 36 months data retention period.
EOP-011-1	R5.	Since Last Compliance Audit	Rolling 36 months data retention period.
EOP-011-1	R6.	Since Last Compliance Audit	Rolling 36 months data retention period.
FAC-003-4	R1.	Last 3 Calendar Years	Rolling 36 Months data retention period.
FAC-003-4	R2.	Last 3 Calendar Years	Rolling 36 Months data retention period.
FAC-014-2	R5.	Last 3 Calendar Years	Rolling 36 Months data retention period.
IRO-001-4	R1.	Most Recent 90-Calendar Days Voice, Most Recent 12 Calendar Months Documentation	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-001-4	R2.	Most Recent 90-Calendar Days Voice, Most Recent 12 Calendar Months Documentation	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
IRO-001-4	R3.	Most Recent 90-Calendar Days Voice, Most Recent 12 Calendar Months Documentation	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-002-5	R2.	Current In-Force Documents and Previous Documents Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
IRO-002-5	R4.	Current In-Force Documents and Previous Documents Since Last Compliance Audit	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
IRO-002-5	R5.	Current Plus 1 Previous Calendar Year	Rolling 12 months data retention period.
IRO-002-5	R6.	Current Plus 1 Previous Calendar Year	Rolling 12 months data retention period.
IRO-006-5	R1.	Last 12 Calendar Months Plus Current Month	Rolling 12 months data retention period.
IRO-008-2	R4.	Rolling 30-Days	Rolling 30-day data retention period.
IRO-008-2	R5.	Rolling 90-Calendar Days for Voice, 12 Months for Operating Logs	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-009-2	R2.	Rolling 12-Month Period	Rolling 12 months data retention period.
IRO-009-2	R3.	Rolling 12-Month Period	Rolling 12 months data retention period.
IRO-009-2	R4.	Rolling 12-Month Period	Rolling 12 months data retention period.
IRO-014-3	R4.	Rolling 90-Calendar Days for Voice, 12 Months for Operating Logs	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-014-3	R5.	Last 12 Calendar Months	Rolling 12 months data retention period.
IRO-014-3	R6.	Current Plus 3 Previous Calendar Years	Rolling 36 Months data retention period.
IRO-014-3	R7.	Rolling 90-Calendar Days for Voice, 12 Months for Operating Logs	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-018-1(i)	R1.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
MOD-027-1	R2.	Last Load Control or Active Power/Frequency Control System Model Verification	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
MOD-027-1	R5.	Last 3 Calendar Years	Rolling 36 Months data retention period.
NUC-001-3	R4.	Current Plus 2 Previous Calendar Years	Rolling 12 months data retention period.
NUC-001-3	R5.	Current Plus 2 Previous Calendar Years	Rolling 12 months data retention period.
NUC-001-3	R7.	Current Plus 2 Previous Calendar Years	Rolling 12 months data retention period.
NUC-001-3	R8.	Current Plus 2 Previous Calendar Years	Rolling 12 months data retention period.

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
PER-003-1	R1.	Three Years or Since Last Compliance Audit Whichever is Longer	Rolling 36 Months data retention period.
PER-003-1	R2.	Three Years or Since Last Compliance Audit Whichever is Longer	Rolling 36 Months data retention period.
PER-003-1	R3.	Three Years or Since Last Compliance Audit Whichever is Longer	Rolling 36 Months data retention period.
PER-004-2	R1.	Current Plus 2 Previous Calendar Years	Rolling 36 Months data retention period.
PER-004-2	R2.	Current Plus 2 Previous Calendar Years	Rolling 36 Months data retention period.
PER-005-3	R3.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-001-1.1(ii)	R1.	Current In-Force Documents	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
PRC-001-1.1(ii)	R4.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-001-1.1(ii)	R5.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-004-5(i)	R1.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-004-5(i)	R2.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-004-5(i)	R3.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-004-5(i)	R4.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-004-5(i)	R5.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-004-5(i)	R6.	Last 12 Calendar Months	Rolling 12 months data retention period.
PRC-005-1.1b	R1.	Three Calendar Years	Rolling 36 Months data retention period.
PRC-005- 6	R3.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-005- 6	R4.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R10.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R15.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R3.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R4.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R5.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-006-3	R9.	Since Last Compliance Audit	Rolling 36 months data retention period.
PRC-010-2	R1.	Six Calendar Years	Rolling 36 months data retention period.
PRC-010-2	R2.	Six Calendar Years	Rolling 36 months data retention period.

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
PRC-017-1	R1.	None Specified	Rolling 36 months data retention period.
PRC-023-4	R1.	Last 3 Calendar Years	Rolling 36 Months data retention period.
PRC-023-4	R2.	Last 3 Calendar Years	Rolling 36 Months data retention period.
PRC-023-4	R6.	Most Recent List of Circuits	Rolling 12 months data retention period.
PRC-025- 2	R1.	Last 3 Calendar Years	Rolling 36 Months data retention period.
PRC-026-1	R2.	Last 12 Calendar Months	Rolling 12 months data retention period.
TOP-001-4	R1.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R2.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R3.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R4.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R5.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R6.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R7.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R8.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R10.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.

Reliability Standard	Req.	Current Evidence Retention Summary	New Evidence Retention Recommendation
TOP-001-4	R11.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R12.	Three Calendar Years	Rolling 36 Months data retention period.
TOP-001-4	R13.	Rolling 30-Days	Rolling 30-day data retention period.
TOP-001-4	R14.	Three Calendar Years	Rolling 36 Months data retention period.
TOP-001-4	R16.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R17.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R18.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-001-4	R20.	Current Plus 1 Previous Calendar Year	Rolling 12 months data retention period.
TOP-001-4	R23.	Current Plus 1 Previous Calendar Year	Rolling 12 months data retention period.
TOP-010-1(i)	R1.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TOP-010-1(i)	R2.	Current Calendar Year Plus One Previous Calendar Year, Except operator logs and voice recordings - retain for 90 calendar days	Rolling 12 months data retention period.
TPL-001-4	R1.	Current and Previous Planning Assessment	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
TPL-001-4	R2.	Since Last Compliance Audit	Rolling 36 Months data retention period.
TPL-007-1	R4.	Current GMD Vulnerability Assessment and Preceding Assessment	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
TPL-007-1	R7.	Five Calendar Years	Rolling 36 months data retention period.
VAR-001-5	R1.	Last 12 Calendar Months	Rolling 12 months data retention period.
VAR-001-5	R2.	Last 12 Calendar Months	Rolling 12 months data retention period.
VAR-001-5	R3.	Last 12 Calendar Months	Rolling 12 months data retention period.

Appendix D: Comparison of Requirements, Measures, Retention Detail and Recommended Retention

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
BAL-002-3	R1.	The Responsible Entity experiencing a Reportable Balancing Contingency Event shall: [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 1.1. within the Contingency Event Recovery Period, demonstrate recovery by returning its Reporting ACE to at least the recovery value of: zero (if its Pre-Reporting Contingency Event ACE Value was positive or equal to zero); however, any Balancing Contingency Event that occurs during the Contingency Event Recovery Period shall reduce the required recovery: (i) beginning at the time of, and (ii) by the magnitude of, such individual Balancing Contingency Event, or, its Pre-Reporting Contingency Event ACE Value (if its Pre-Reporting Contingency Event ACE Value was negative); however, any Balancing Contingency Event that occurs during the Contingency Event Recovery Period shall reduce the required recovery: (i) beginning at the time of, and (ii) by the magnitude of, such individual Balancing Contingency Event. 1.2. document all Reportable Balancing Contingency Events using CR Form 1. 1.3. deploy Contingency Reserve, within system constraints, to respond to all Reportable Balancing Contingency Events, however, it is not subject to compliance with Requirement R1 part 1.1 if the Responsible Entity: 1.3.1 is (i) a Balancing Authority or (ii) a Reserve	Each Responsible Entity shall have, and provide upon request, as evidence, a CR Form 1 with date and time of occurrence to show compliance with Requirement R1. If Requirement R1 part 1.3 applies, then dated documentation that demonstrates compliance with Requirement R1 part 1.3 must also be provided.	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.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Sharing Group with at least one member that: is experiencing a Reliability Coordinator declared Energy Emergency Alert Level, and is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan, and has depleted its Contingency Reserve to a level below its Most Severe Single Contingency, and has, during communications with its Reliability Coordinator in accordance with the Energy Emergency Alert procedures, (i) notified the Reliability Coordinator of the conditions described in the preceding two bullet points preventing the Responsible Entity from complying with Requirement R1 part 1.1, and (ii) provided the Reliability Coordinator with an ACE recovery plan, including target recovery time or, 1.3.2 the Responsible Entity experiences: multiple Contingencies where the combined MW loss exceeds its Most Severe Single Contingency and that are defined as a single Balancing Contingency Event, or multiple Balancing Contingency Events within the sum of the time periods defined by the Contingency Event Recovery Period and Contingency Reserve Restoration Period whose combined magnitude exceeds the Responsible Entity's Most Severe Single Contingency.			
BAL-002-3	R2.	Each Responsible Entity shall develop, review and maintain annually, and implement an Operating Process as part of its Operating Plan to determine its Most Severe Single Contingency and make preparations to have Contingency Reserve equal to, or greater than the Responsible Entity's Most Severe Single Contingency available for maintaining system reliability. [Violation Risk Factor: High] [Time Horizon: Operations Planning]	Each Responsible Entity will have the following documentation to show compliance with Requirement R2: • a dated Operating Process; • evidence to indicate that the Operating Process has been reviewed and maintained annually; and, • evidence such as Operating Plans or other operator documentation that demonstrate that the entity determines its Most Severe Single Contingency and that Contingency Reserves equal to or greater than its Most Severe Single	The Responsible Entity shall retain data or evidence to show compliance for the current year, plus three previous calendar years, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			Contingency are included in this process.		
BAL-003-1.1	R1.	Each Frequency Response Sharing Group (FRSG) or Balancing Authority that is not a member of a FRSG shall achieve an annual Frequency Response Measure (FRM) (as calculated and reported in accordance with Attachment A) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each FRSG or BA that is not a member of a FRSG to maintain Interconnection Frequency Response equal to or more negative than the Interconnection Frequency Response Obligation. [Risk Factor: High][Time Horizon: Real-time Operations]	Each Frequency Response Sharing Group or Balancing Authority that is not a member of a Frequency Response Sharing Group shall have evidence such as dated data plus documented formula in either hardcopy or electronic format that it achieved an annual FRM (in accordance with the methods specified by the ERO in Attachment A with data from FRS Form 1 reported to the ERO as specified in Attachment A) that is equal to or more negative than its FRO to demonstrate compliance with Requirement R1.	The BA shall retain data or evidence to show compliance with Requirements R1-R4, for the current year plus the previous three calendar years.	Rolling 36 months data retention period.
CIP-002-5.1a	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.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.	Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.	Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.	Rolling 36 months data retention period.
CIP-014-2	R1.	Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses	Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of	Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. [VRF: High; Time-Horizon: Long-term Planning] 1.1. Subsequent risk assessments shall be performed: · At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or · At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.	acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.		
COM-001-3	R1.	Each Reliability Coordinator shall have Interpersonal Communication capability with the following entities (unless the Reliability Coordinator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): [Violation Risk Factor: High] [Time Horizon: Real-time Operations]1.1. All Transmission Operators and Balancing Authorities within its Reliability Coordinator Area.1.2. Each adjacent Reliability	Each Reliability Coordinator shall have and provide upon request evidence that it has Interpersonal Communication capability with all Transmission Operators and Balancing Authorities within its Reliability Coordinator Area and with each adjacent Reliability Coordinator within the same Interconnection, which could include, but is not limited to: • physical assets, or • dated evidence, such as, equipment	The Reliability Coordinator for Requirements R1, R2, R9, and R10, Measures M1, M2, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Coordinator within the same Interconnection.	specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R1.)		
COM-001-3	R2.	Each Reliability Coordinator shall designate an Alternative Interpersonal Communication capability with the following entities: [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 2.1. All Transmission Operators and Balancing Authorities within its Reliability Coordinator Area. 2.2. Each adjacent Reliability Coordinator within the same Interconnection.	Each Reliability Coordinator shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with all Transmission Operators and Balancing Authorities within its Reliability Coordinator Area and with each adjacent Reliability Coordinator within the same Interconnection, which could include, but is not limited to: • physical assets, or • dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R2.)	The Reliability Coordinator for Requirements R1, R2, R9, and R10, Measures M1, M2, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-001-3	R12.	Each Reliability Coordinator, Transmission Operator, Generator Operator, and Balancing Authority shall have internal Interpersonal Communication capabilities for the exchange of information that is necessary for the Reliable Operation of the BES. [Violation Risk Factor: High] [Time Horizon: Real-time Operations].	Each Reliability Coordinator, Transmission Operator, Generator Operator, and Balancing Authority shall have and provide upon request evidence that it has internal Interpersonal Communication capability, which could include, but is not limited to: • physical assets, or • dated evidence, such as, equipment specifications and installation documentation, operating procedures, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications.	Responsible entities under Requirement R12, Measure M12 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-001-3	R3.	Each Transmission Operator shall have Interpersonal Communication capability with the following entities (unless the Transmission Operator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 3.1. Its Reliability	Each Transmission Operator shall have and provide upon request evidence that it has Interpersonal Communication capability with its Reliability Coordinator, each Balancing Authority, Distribution Provider, and Generator Operator within its Transmission Operator Area, and each adjacent	The Transmission Operator for Requirements R3, R4, R9, and R10, Measures M3, M4, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Coordinator. 3.2. Each Balancing Authority within its Transmission Operator Area. 3.3. Each Distribution Provider within its Transmission Operator Area. 3.4. Each Generator Operator within its Transmission Operator Area. 3.5. Each adjacent Transmission Operator synchronously connected. 3.6. Each adjacent Transmission Operator asynchronously connected.	Transmission Operator asynchronously or synchronously connected, which could include, but is not limited to: • Physical assets, or • Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communication. (R3.)		
COM-001-3	R4.	Each Transmission Operator shall designate an Alternative Interpersonal Communication capability with the following entities: [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 4.1. Its Reliability Coordinator. 4.2. Each Balancing Authority within its Transmission Operator Area. 4.3. Each adjacent Transmission Operator synchronously connected. 4.4. Each adjacent Transmission Operator asynchronously connected.	Each Transmission Operator shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with its Reliability Coordinator, each Balancing Authority within its Transmission Operator Area, and each adjacent Transmission Operator asynchronously and synchronously connected, which could include, but is not limited to: • Physical assets, or • Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R4.)	The Transmission Operator for Requirements R3, R4, R9, and R10, Measures M3, M4, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-001-3	R5.	Each Balancing Authority shall have Interpersonal Communication capability with the following entities (unless the Balancing Authority detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply): [Violation Risk Factor: High] [Time Horizon: Real-time Operations]5.1. Its Reliability Coordinator.5.2. Each Transmission Operator that operates Facilities within its Balancing Authority Area.5.3. Each Distribution Provider within its Balancing Authority Area.5.4. Each Generator Operator that operates Facilities within its Balancing Authority Area.5.5. Each Adjacent Balancing Authority.	Each Balancing Authority shall have and provide upon request evidence that it has Interpersonal Communication capability with its Reliability Coordinator, each Transmission Operator and Generator Operator that operates Facilities within its Balancing Authority Area, each Distribution Provider within its Balancing Authority Area, and each adjacent Balancing Authority, which could include, but is not limited to: • Physical assets, or • Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice	The Balancing Authority for Requirements R5, R6, R9, and R10, Measures M5, M6, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			recordings, or electronic communications. (R5.)		
COM-001-3	R6.	Each Balancing Authority shall designate an Alternative Interpersonal Communication capability with the following entities: [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 6.1. Its Reliability Coordinator. 6.2. Each Transmission Operator that operates Facilities within its Balancing Authority Area. 6.3. Each Adjacent Balancing Authority.	Each Balancing Authority shall have and provide upon request evidence that it designated an Alternative Interpersonal Communication capability with its Reliability Coordinator, each Transmission Operator that operates Facilities within its Balancing Authority Area, and each adjacent Balancing Authority, which could include, but is not limited to: • Physical assets, or • Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R6.)	The Balancing Authority for Requirements R5, R6, R9, and R10, Measures M5, M6, M9, and M10 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-001-3	R8.	Each Generator Operator shall have Interpersonal Communication capability with the following entities (unless the Generator Operator detects a failure of its Interpersonal Communication capability in which case Requirement R11 shall apply): [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 8.1. Its Balancing Authority. 8.2. Its Transmission Operator.	Each Generator Operator shall have and provide upon request evidence that it has Interpersonal Communication capability with its Balancing Authority and its Transmission Operator, which could include, but is not limited to: • Physical assets, or • Dated evidence, such as, equipment specifications and installation documentation, test records, operator logs, voice recordings, transcripts of voice recordings, or electronic communications. (R8.)	The Generator Operator for Requirements R8 and R11, Measures M8 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-002-4	R5.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: Confirm the receiver's response if the repeated information is correct (in accordance with Requirement R6). • Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver, or • Take an alternative action if a response is not received or if the Operating Instruction	Each Reliability Coordinator, Transmission Operator, and Balancing Authority that issued an oral two-party, person-to-person Operating Instruction during an Emergency, excluding oral single-party to multiple-party burst Operating Instructions, shall have evidence that the issuer either: 1) confirmed that the response from the recipient of the Operating Instruction was correct; 2) reissued the Operating Instruction if the repeated information was incorrect or if requested by the receiver; or 3) took an alternative action if a	The Generator Operator for Requirements R8 and R11, Measures M8 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		was not understood by the receiver.	response was not received or if the Operating Instruction was not understood by the receiver. Such evidence could include, but is not limited to, dated and timestamped voice recordings, or dated and time-stamped transcripts of voice recordings, or dated operator logs in fulfillment of Requirement R5.		
COM-002-4	R6.	Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that receives an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: • Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct, or• Request that the issuer reissue the Operating Instruction.	Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that was the recipient of an oral two-party, person-to-person Operating Instruction during an Emergency, excluding oral single-party to multipleparty burst Operating Instructions, shall have evidence to show that the recipient either repeated, not necessarily verbatim, the Operating Instruction and received confirmation from the issuer that the response was correct, or requested that the issuer reissue the Operating Instruction in fulfillment of Requirement R6. Such evidence may include, but is not limited to, dated and time-stamped voice recordings (if the entity has such recordings), dated operator logs, an attestation from the issuer of the Operating Instruction, memos or transcripts.	The Generator Operator for Requirements R8 and R11, Measures M8 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
COM-002-4	R7.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues a written or oral single-party to multiple-party burst Operating Instruction during an Emergency shall confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction.	Each Balancing Authority, Reliability Coordinator and Transmission Operator that issued a written or oral single or multiple-party burst Operating Instruction during an Emergency shall provide evidence that the Operating Instruction was received by at least one receiver. Such evidence may include, but is not limited to, dated and timestamped voice recordings (if the entity has such recordings), dated operator logs, electronic records, memos or transcripts.	The Generator Operator for Requirements R8 and R11, Measures M8 and M11 shall retain written documentation for the most recent twelve calendar months and voice recordings for the most recent 90 calendar days.	Rolling 12 months data retention period.
EOP-005-3	R1.	Each Transmission Operator shall develop and implement	M1. M2. M3. M4. M5. M6. M7. M8. M9. Each	Approved restoration plan and any restoration plans in effect	Current plan, model, agreement,

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shutdown area to service. The restoration plan shall include: [Violation Risk Factor = High] [Time Horizon = Operations Planning, Real-time Operations]1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.1.6. Identification of acceptable operating voltage and frequency limits during restoration.1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units	Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator and will have evidence, such as operator logs, voice recordings or other operating documentation, voice recordings or other communication documentation to show that its restoration plan was implemented for times when a Disturbance has occurred, in accordance with Requirement R1.	since the last compliance audit for Requirement R1, Measure M1.	methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.			
EOP-006-3	R1.	Each Reliability Coordinator shall develop, maintain, and implement a Reliability Coordinator Area restoration plan. The scope of the Reliability Coordinator's restoration plan starts when Blackstart Resources are utilized to re-energize a shutdown area of the Bulk Electric System (BES), or separation has occurred between neighboring Reliability Coordinators, or an energized island has been formed on the BES within the Reliability Coordinator Area. The scope of the Reliability Coordinator's restoration plan ends when all of its Transmission Operators are interconnected and its Reliability Coordinator Area is connected to all of its neighboring Reliability Coordinator Areas. The restoration plan shall include: [Violation Risk Factor = High] [Time Horizon = Operations Planning, Real-time Operations]1.1. A description of the high-level strategy to be employed during restoration events for restoring the Interconnection, including minimum criteria for meeting the objectives of the Reliability Coordinator's restoration plan.1.2. Criteria and conditions for re-establishing interconnections with other Transmission Operators within its Reliability Coordinator Area, with adjacent Transmission Operators in other Reliability Coordinator Areas, and with adjacent Reliability Coordinators.1.3. Reporting requirements for the entities within the Reliability Coordinator Area during a restoration event.1.4. Criteria for sharing information regarding restoration with	Each Reliability Coordinator shall have available a dated copy of its restoration plan and will have evidence, such as operator logs or other operating documentation, voice recordings, or other communication documentation to show that its restoration plan was implemented in accordance with Requirement R1.	The current restoration plan and any restoration plans in effect since the last compliance audit for Requirement R1, Measure M1.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		neighboring Reliability Coordinators and with Transmission Operators and Balancing Authorities within its Reliability Coordinator Area.1.5. Identification of the Reliability Coordinator as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators, and to Transmission Operators, and Balancing Authorities within its Reliability Coordinator Area.1.6. Criteria for transferring operations and authority back to the Balancing Authority.			
EOP-008-2	R3.	Each Reliability Coordinator shall have a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that depend on primary control center functionality. To avoid requiring a tertiary facility, a backup facility is not required during: [Violation Risk Factor = High] [Time Horizon = Operations Planning]• Planned outages of the primary or backup facilities of two weeks or less• Unplanned outages of the primary or backup facilities	Each Reliability Coordinator shall provide dated evidence that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Requirement R3.	Each Reliability Coordinator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it has a backup control center facility (provided through its own dedicated backup facility or at another entity's control center staffed with certified Reliability Coordinator operators when control has been transferred to the backup facility) in accordance with Requirement R3 that provides the functionality required for maintaining compliance with all Reliability Standards that are applicable to the primary control center functionality in accordance with Measurement M3.	Rolling 36 months data retention period.
EOP-008-2	R4.	Each Balancing Authority and Transmission Operator shall have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that depend on a Balancing Authority and Transmission Operator's primary control center functionality respectively. To avoid requiring tertiary	Each Balancing Authority and Transmission Operator shall provide dated evidence that its backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's or Transmission Operator's primary control center	Each Balancing Authority and Transmission Operator shall retain dated evidence for the time period since its last compliance audit, that it has demonstrated that it's backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) in accordance with Requirement R4 includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		functionality, backup functionality is not required during: [Violation Risk Factor = High] [Time Horizon = Operations Planning] • Planned outages of the primary or backup functionality of two weeks or less • Unplanned outages of the primary or backup functionality	functionality in accordance with Requirement R4.	center functionality in accordance with Measurement M4.	
EOP-011-1	R1.	Each Transmission Operator shall develop, maintain and implement a Reliability Coordinator-approved Emergency Operating Plan to mitigate operating Emergencies on its Transmission System. At a minimum, the Emergency Operating Plan shall include the following elements: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning]	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.	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.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-011-1	R2.	Each Balancing Authority shall develop, maintain, and implement a Reliability Coordinator-approved Emergency Operating Plan to mitigate Capacity and Energy Emergencies. At a minimum, the Emergency Operating Plan shall include the following elements: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning]	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.	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.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
EOP-011-1	R3.	Each Reliability Coordinator shall approve or disapprove, with stated reasons for disapproval, Emergency Operating Plans submitted by Transmission Operators and Balancing Authorities within 30 calendar days of submittal. [Violation Risk Factor: Medium] [Time	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.	The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Horizon: Operations Planning]			
EOP-011-1	R4.	Each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority shall notify, as soon as practical, other impacted Reliability Coordinators, Balancing Authorities and Transmission Operators. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	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.	The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.	Rolling 36 months data retention period.
EOP-011-1	R5.	Each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall initiate an Energy Emergency Alert, as detailed in Attachment 1. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	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.	The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.	Rolling 36 months data retention period.
EOP-011-1	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]	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.	The Reliability Coordinator shall maintain evidence of compliance since the last audit for Requirements R3, R5, and R6 and Measures M3, M5, and M6.	Rolling 36 months data retention period.
FAC-003-4	R1.	Each applicable Transmission Owner and applicable Generator Owner	Each applicable Transmission Owner and applicable Generator	The applicable Transmission Owner and applicable Generator Owner retains data	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		shall manage vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) of its applicable line(s) which are either an element of an IROL, or an element of a Major WECC Transfer Path; operating within their Rating and all Rated Electrical Operating Conditions of the types shown below4 [Violation Risk Factor: High] [Time Horizon: Real-time] 1.1 An encroachment into the MVCD as shown in FAC-003-Table 2, observed in Real-time, absent a Sustained Outage, 1.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,6 1.3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage7, 1.4. An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.	Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R1. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R1)	or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.	
FAC-003-4	R2.	Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the MVCD of its applicable line(s) which are not either an element of an IROL, or an element of a Major WECC Transfer Path; operating within its Rating and all Rated Electrical Operating Conditions of the types shown below [Violation Risk Factor: High] [Time Horizon: Real-time] 2.1. An encroachment into the MVCD, observed in Real-time, absent a Sustained Outage, 2.2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage, 2.3. An encroachment due to blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained	Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R2. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments. (R2)	The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Outage, 2.4. An encroachment due to vegetation growth into the line MVCD that caused a vegetation-related Sustained Outage.			
FAC-014-2	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows: The Reliability Coordinator shall provide its SOLs (including the subset of SOLs that are IROLs) to adjacent Reliability Coordinators and Reliability Coordinators who indicate a reliability-related need for those limits, and to the Transmission Operators, Transmission Planners, Transmission Service Providers and Planning Authorities within its Reliability Coordinator Area. For each IROL, the Reliability Coordinator shall provide the following supporting information:	See R2. Measure	The applicable Transmission Owner and applicable Generator Owner retains data or evidence to show compliance with Requirements R1, R2, R3, R5, R6 and R7, for three calendar years.	Rolling 36 Months data retention period.
IRO-001-4	R1.	Each Reliability Coordinator shall act, or direct others to act, by issuing Operating Instructions, to ensure the reliability of its Reliability Coordinator Area. [Violation Risk Factor: High][Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Reliability Coordinator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to address the reliability of its Reliability Coordinator Area via direct actions or by issuing Operating Instructions.	The Reliability Coordinator for Requirement R1, Measure M1 shall retain voice recordings for the most recent 90-calendar days and documentation for the most recent 12-calendar months.	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-001-4	R2.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall comply with its Reliability Coordinator's Operating Instructions unless compliance with the Operating Instructions cannot be physically implemented or unless such actions would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or	The Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider for Requirements R2 and R3, Measures M2 and M3 shall retain voice recordings for the most recent 90-calen dar days and documentation for the most recent 12-calendar months.	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	equivalent documentation, that will be used to determine that it complied with its Reliability Coordinator's Operating Instructions, unless the instruction could not be physically implemented, or such actions would have violated safety, equipment, regulatory or statutory requirements. In such cases, the Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider shall have and provide copies of the safety, equipment, regulatory, or statutory requirements as evidence for not complying with the Reliability Coordinator's Operating Instructions. If such a situation has not occurred, the Transmission Operator, Balancing Authority, Generator Operator, or Distribution Provider may provide an attestation.		
IRO-001-4	R3.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall inform its Reliability Coordinator of its inability to perform the Operating Instruction issued by its Reliability Coordinator in Requirement R1. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it informed its Reliability Coordinator of its inability to perform an Operating Instruction issued by its Reliability Coordinator in Requirement R1.	The Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider for Requirements R2 and R3, Measures M2 and M3 shall retain voice recordings for the most recent 90-calendar days and documentation for the most recent 12-calendar months.	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.
IRO-002-5	R2.	Each Reliability Coordinator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing its Real-time	Each Reliability Coordinator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Reliability	The Reliability Coordinator shall retain its current, in force document and any documents in force for the current year and previous calendar year for Requirements R1, R2, and R4 and Measures M1, M2, and M4.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		monitoring and Real-time Assessments. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, as specified in the requirement.		
IRO-002-5	R4.	Each Reliability Coordinator shall provide its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Reliability Coordinator shall have, and provide upon request evidence that could include, but is not limited to, a documented procedure or equivalent evidence that will be used to confirm that the Reliability Coordinator has provided its System Operators with the authority to approve planned outages and maintenance of its telecommunication, monitoring and analysis capabilities.	The Reliability Coordinator shall retain its current, in force document and any documents in force for the current year and previous calendar year for Requirements R1, R2, and R4 and Measures M1, M2, and M4.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
IRO-002-5	R5.	Each Reliability Coordinator shall monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	Each Reliability Coordinator shall monitor Facilities, the status of Remedial Action Schemes, and non-BES facilities identified as necessary by the Reliability Coordinator, within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to identify any System Operating Limit exceedances and to determine any Interconnection Reliability Operating Limit exceedances within its Reliability Coordinator Area. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	The Reliability Coordinator shall keep data or evidence for Requirements R5 and R6 and Measures M5 and M6 for the current calendar year and one previous calendar year.	Rolling 12 months data retention period.
IRO-002-5	R6.	Each Reliability Coordinator shall have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	Each Reliability Coordinator shall have monitoring systems that provide information utilized by the Reliability Coordinator's operating personnel, giving particular emphasis to alarm management and awareness systems, automated data transfers, and synchronized information systems, over a redundant infrastructure. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	The Reliability Coordinator shall keep data or evidence for Requirements R5 and R6 and Measures M5 and M6 for the current calendar year and one previous calendar year.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
IRO-006-5	R1.	Each Reliability Coordinator and Balancing Authority that receives a request pursuant to an Interconnection-wide transmission loading relief procedure (such as Eastern Interconnection TLR, WECC Unscheduled Flow Mitigation, or congestion management procedures from the ERCOT Protocols) from any Reliability Coordinator, Balancing Authority, or Transmission Operator in another Interconnection to curtail an Interchange Transaction that crosses an Interconnection boundary shall comply with the request, unless it provides a reliability reason to the requestor why it cannot comply with the request.	Each Reliability Coordinator and Balancing Authority shall provide evidence (such as dated logs, voice recordings, Tag histories, and studies, in electronic or hard copy format) that, when a request to curtail an Interchange Transaction crossing an Interconnection boundary pursuant to an Interconnection-wide transmission loading relief procedure was made from another Reliability Coordinator, Balancing Authority, or Transmission Operator in that other Interconnection, it complied with the request or provided a reliability reason why it could not comply with the request (R1).	The Reliability Coordinator and Balancing Authority shall maintain evidence to show compliance with R1 for the most recent twelve calendar months plus the current month.	Rolling 12 months data retention period.
IRO-008-2	R4.	Each Reliability Coordinator shall ensure that a Real-time Assessment is performed at least once every 30 minutes. [Violation Risk Factor: High] [Time Horizon: Same-day Operations, Real-time Operations]	Each Reliability Coordinator shall have, and make available upon request, evidence to show it ensured that a Real-time Assessment is performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.	Each Reliability Coordinator shall each keep data or evidence for Requirement R4 and Measure M4 for a rolling 30-calendar day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 30-day data retention period.
IRO-008-2	R5.	Each Reliability Coordinator shall notify impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, when the results of a Real-time Assessment indicate an actual or expected condition that results in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Reliability Coordinator Wide Area. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	Each Reliability Coordinator shall make available upon request, evidence that it informed impacted Transmission Operators and Balancing Authorities within its Reliability Coordinator Area, and other impacted Reliability Coordinators as indicated in its Operating Plan, of its actual or expected operations that result in, or could result in, a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) exceedance within its Wide Area. Such evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence. If such a situation has not occurred, the Reliability	Each Reliability Coordinator shall keep data or evidence to show compliance for Requirements R1 through R3, R5, and R6 and Measures M1 through M3, M5, and M6 for a rolling 90-calendar days period for analyses, the most recent 90- calendar days for voice recordings, and 12 months for operating logs and e-mail records unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			Coordinator may provide an attestation.		
IRO-009-2	R2.	Each Reliability Coordinator shall initiate one or more Operating Processes, Procedures, or Plans (not limited to the Operating Processes, Procedures, or Plans developed for Requirement R1) that are intended to prevent an IROL exceedance, as identified in the Reliability Coordinator's Real-time monitoring or Real-time Assessment. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it initiated one or more Operating Processes, Procedures or Plans (not limited to the Operating Processes, Procedures, or Plans developed for Requirements R1) in accordance with Requirement R2. This evidence could include, but is not limited to, Operating Processes, Procedures, or Plans from Requirement R1, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other evidence.	The Reliability Coordinator shall retain evidence of Requirement R1; Requirement R2; Requirement R3; and Requirement R4 for a rolling 12 months.	Rolling 12 months data retention period.
IRO-009-2	R3.	Each Reliability Coordinator shall act or direct others to act so that the magnitude and duration of an IROL exceedance is mitigated within the IROL's Tv, as identified in the Reliability Coordinator's Real-time monitoring or Real-time Assessment. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it acted or directed others to act in accordance with Requirement R3. This evidence could include, but is not limited to, Operating Processes, Procedures, or Plans, dated operating logs, dated voice recordings, dated transcripts of voice recordings, or other evidence.	The Reliability Coordinator shall retain evidence of Requirement R1; Requirement R2; Requirement R3; and Requirement R4 for a rolling 12 months.	Rolling 12 months data retention period.
IRO-009-2	R4.	Each Reliability Coordinator shall operate to the most limiting IROL and Tv in instances where there is a difference in an IROL or its Tv between Reliability Coordinators that are responsible for that Facility (or group of Facilities). [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	Each Reliability Coordinator shall have, and make available upon request, evidence to confirm that it operated to the most limiting IROL and Tv in instances where there was a difference in an IROL or its Tv. Such evidence could include, but is not limited to, dated computer printouts, dated operator logs, dated voice recordings, dated transcripts of voice recordings, or other equivalent evidence in accordance with Requirement R4.	The Reliability Coordinator shall retain evidence of Requirement R1; Requirement R2; Requirement R3; and Requirement R4 for a rolling 12 months.	Rolling 12 months data retention period.
IRO-014-3	R4.	Each impacted Reliability Coordinator shall operate as though the Emergency exists during each instance where Reliability Coordinators disagree on the existence of an Emergency. [Violation	Each Reliability Coordinator shall have and provide evidence which may include but is not limited to operator logs, voice recordings or transcripts of voice	Each Reliability Coordinator shall retain evidence for 90-calendar days for operator logs and voice recordings and for the period since the last compliance audit for other evidence for Requirements R3,	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	recordings, electronic communications, or equivalent documentation, that will be used to determine that it operated as though an Emergency existed during each instance where Reliability Coordinators disagreed on the existence of an Emergency.	R4, and R7 and Measures M3, M4, and M7.	
IRO-014-3	R5.	Each Reliability Coordinator that Identifies an Emergency in its Reliability Coordinator Area shall develop an action plan to resolve the Emergency during those instances where impacted Reliability Coordinators disagree on the existence of an Emergency. [Violation Risk Factor: High][Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Reliability Coordinator that identifies an Emergency in its Reliability Coordinator Area shall have evidence that it developed an action plan during those instances where impacted Reliability Coordinators disagreed on the existence of an Emergency. This evidence may include but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent dated documentation.	Each Reliability Coordinator shall retain its most recent 12 months of evidence for Requirement R5 and Measure M5.	Rolling 12 months data retention period.
IRO-014-3	R6.	Each impacted Reliability Coordinator shall implement the action plan developed by the Reliability Coordinator that identifies the Emergency during those instances where Reliability Coordinators disagree on the existence of an Emergency, unless such actions would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High][Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each impacted Reliability Coordinator shall have and provide evidence which may include but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent dated documentation, that will be used to determine that it implemented the action plan developed by the Reliability Coordinator who identifies the Emergency when Reliability Coordinators disagree on the existence of an Emergency unless such actions would have violated safety, equipment, regulatory, or statutory requirements.	Each Reliability Coordinator shall retain 3-calendar years plus current calendar year of evidence for Requirement R6 and Measure M6.	Rolling 36 Months data retention period.
IRO-014-3	R7.	Each Reliability Coordinator shall assist Reliability Coordinators, if requested and able, provided that the requesting Reliability Coordinator has implemented its emergency procedures, unless such actions cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High]	Each Reliability Coordinator shall make available upon request, evidence that requested assistance was provided, if able, to requesting Reliability Coordinators unless such actions could not be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. Such	Each Reliability Coordinator shall retain evidence for 90-calendar days for operator logs and voice recordings and for the period since the last compliance audit for other evidence for Requirements R3, R4, and R7 and Measures M3, M4, and M7.	Rolling 3 Months data retention period for voice and audio recordings and 12 months for operating logs.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		[Time Horizon: Real-time Operations]	evidence could include but is not limited to dated operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence in electronic or hard copy format. If such a situation has not occurred, the Reliability Coordinator may provide an attestation.		
IRO-018-1(i)	R1.	Each Reliability Coordinator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: [Violation Risk Factor: High] [Time Horizon: Real-time Operations]1.1. Criteria for evaluating the quality of Real-time data;1.2. Provisions to indicate the quality of Real-time data to the System Operator; and1.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.	Each Reliability Coordinator shall have evidence it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Reliability Coordinator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator or supporting logs, dated checklists, voice recordings, voice transcripts, or other evidence.	The Reliability Coordinator shall retain evidence of compliance for Requirements R1 and R3 and Measures M1 and M3 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
MOD-027-1	R2.	Each Generator Owner shall provide, for each applicable unit, a verified turbine/governor and load control or active power/frequency control model, including documentation and data (as specified in Part 2.1) to its Transmission Planner in accordance with the periodicity specified in MOD-027 Attachment 1. 2.1. Each applicable unit's model shall be verified by the Generator Owner using one or more models acceptable to the Transmission Planner. Verification for individual units rated less than 20 MVA (gross nameplate rating) in a generating plant (per Section 4.2.1.2, 4.2.2.2, or 4.2.3.2) may be performed using either individual unit or	The Generator Owner must have and provide dated evidence it verified each generator turbine/governor and load control or active power/frequency control model according to Part 2.1 for each applicable unit and a dated transmittal (e.g., electronic mail message, postal receipt, or confirmation of facsimile) as evidence it provided the model, documentation, and data to its Transmission Planner, in accordance with Requirement R2.	The Generator Owner shall retain the latest turbine/governor and load control or active power/frequency control system model verification evidence of Requirement R2, Measure M2.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		aggregate unit model(s) or both. Each verification shall include the following: 2.1.1. Documentation comparing the applicable unit's MW model response to the recorded MW response for either: • A frequency excursion from a system disturbance that meets MOD-027 Attachment 1 Note 1 with the applicable unit on-line, • A speed governor reference change with the applicable unit on-line, or • A partial load rejection test, 2.1.2. Type of governor and load control or active power control/frequency control1 equipment, 2.1.3. A description of the turbine (e.g. for hydro turbine - Kaplan, Francis, or Pelton; for steam turbine - boiler type, normal fuel type, and turbine type; for gas turbine - the type and manufacturer; for variable energy plant - type and manufacturer), 2.1.4. Model structure and data for turbine/governor and load control or active power/frequency control, and 2.1.5. Representation of the real power response effects of outer loop controls (such as operator set point controls, and load control but excluding AGC control) that would override the governor response (including blocked or nonfunctioning governors or modes of operation that limit Frequency Response), if applicable.			
MOD-027-1	R5.	Each Transmission Planner shall provide a written response to the Generator Owner within 90 calendar days of receiving the turbine/governor and load control or active power/frequency control system verified model information in accordance with Requirement R2 that the model is usable (meets the criteria specified in Parts 5.1 through 5.3) or is not usable. 5.1. The turbine/governor and load control or active power/frequency control function model initializes to compute modeling data without error,5.2. A no-	Evidence of Requirement R5 must include, for each model received, the dated response indicating the model was usable or not usable according to the criteria specified in Parts 5.1 through 5.3 and for a model that is not useable, a technical description is the model is not usable, and dated evidence of transmittal (e.g., electronic mail messages, postal receipts, or confirmation of facsimile) that the Generator Owner was notified within 90 calendar days of receipt of model	The Transmission Planner shall retain the information/data request and provided response evidence of Requirements R1 and R5, Measures M1 and M5 for 3 calendar years from the date the document was provided.	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		disturbance simulation results in negligible transients, and5.3. For an otherwise stable simulation, a disturbance simulation results in the turbine/governor and load control or active power/frequency control model exhibiting positive damping.If the model is not usable, the Transmission Planner shall provide a technical description of why the model is not usable.	information in accordance with Requirement R5.		
NUC-001-3	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall [Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-time Operations]	Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority: · The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1) · The electric system was operated to meet the NPIRs. (Requirement 4.2) · The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs	For Measures 4, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.	Rolling 12 months data retention period.
NUC-001-3	R5.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall operate the nuclear plant to meet the NPIRs. [Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-time Operations]	The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the nuclear power plant is being operated consistent with the NPIRs.	For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.	Rolling 12 months data retention period.
NUC-001-3	R7.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs. [Violation Risk Factor: High] [Time Horizon: Long-term Planning]	The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the Transmission Entities to meet the NPIRs.	For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
NUC-001-3	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs. [Violation Risk Factor: High] [Time Horizon: Long-term Planning]	The Transmission Entities shall each provide evidence that the entities informed the Nuclear Plant Generator Operator of changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs.	For Measures 4, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.	Rolling 12 months data retention period.
PER-003-1	R1.	Each Reliability Coordinator shall staff its Real-time operating positions performingReliability Coordinator reliability-related tasks with System Operators who havedemonstrated minimum competency in the areas listed by obtaining and maintaining avalid NERC Reliability Operator certificate (11.1. Areas of Competency) : [Risk Factor: High][Time Horizon:Real-time Operations]1.1.1. Resource and demand balancing1.1.2. Transmission operations1.1.3. Emergency preparedness and operations1.1.4. System operations1.1.5. Protection and control1.1.6. Voltage and reactive1.1.7. Interchange scheduling and coordination1.1.8. Interconnection reliability operations and coordination	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate (R1, R2, R3): M1.1 A list of Real-time operating positions.M1.2 A list of System Operators assigned to its Real-time operating positions.M1.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.M1.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall keep data or evidence to show compliance for three years or since its last compliance audit, whichever time frame is the greatest, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 36 Months data retention period.
PER-003-1	R2.	Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates (1 2.1. Areas of Competency) : [Risk Factor: High][Time Horizon:	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate (R1, R2, R3):	Three Years or Since Last Compliance Audit Whichever is Longer	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Real-time Operations]: 2.1.1. Transmission operations 2.1.2. Emergency preparedness and operations 2.1.3. System operations 2.1.4. Protection and control 2.1.5. Voltage and reactive 2.2. Certificates • Reliability Operator • Balancing, Interchange and Transmission Operator • Transmission Operator	M1.1 A list of Real-time operating positions. M1.2 A list of System Operators assigned to its Real-time operating positions. M1.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency. M1.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.		
PER-003-1	R3.	Each Balancing Authority shall staff its Real-time operating positions performingBalancing Authority reliability-related tasks with System Operators who havedemonstrated minimum competency in the areas listed by obtaining and maintainingone of the following valid NERC certificates (1) : [Risk Factor: High][Time Horizon:Real-time Operations]:3.1. Areas of Competency3.1.1. Resources and demand balancing3.1.2. Emergency preparedness and operations3.1.3. System operations3.1.4. Interchange scheduling and coordination3.2. Certificates• Reliability Operator• Balancing, Interchange and Transmission Operator• Balancing and Interchange Operator	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate (R1, R2, R3): M1.1 A list of Real-time operating positions.M1.2 A list of System Operators assigned to its Real-time operating positions.M1.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.M1.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.	Three Years or Since Last Compliance Audit Whichever is Longer	Rolling 36 Months data retention period.
PER-004-2	R1.	Each Reliability Coordinator shall be staffed with adequately trained and NERC-certified Reliability Coordinator operators, 24 hours per day, seven days per week. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	No measures in the Standard.	Each Reliability Coordinator shall keep evidence of compliance for the previous two calendar years plus the current year. If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer. Evidence	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
				used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor. The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.	
PER-004-2	R2.	Reliability Coordinator operating personnel shall place particular attention on SOLs and IROLs and inter-tie facility limits. The Reliability Coordinator shall ensure protocols are in place to allow Reliability Coordinator operating personnel to have the best available information at all times. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	No measures in the Standard.	Each Reliability Coordinator shall keep evidence of compliance for the previous two calendar years plus the current year. If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer. Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor.The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.	Rolling 36 Months data retention period.
PER-005-3	R3.	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System and Automatic Reclosing Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. [Violation Risk Factor: High] [Time Horizon: Operations Planning]	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System and Automatic Reclosing Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.	For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component, or all performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component since the previous scheduled audit date, whichever is longer.	Rolling 36 months data retention period.
PRC-001-1.1(ii)	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of Protection System schemes applied in its area.	Each Generator Operator and Transmission Operator shall have and provide upon request evidence that could include but is not limited to, revised fault analysis study, letters of agreement on settings, notifications of changes, or other equivalent evidence that will be used to confirm that there was coordination	Each Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			of new protective systems or changes as noted in Requirements 3, 3.1, and 3.2.		
PRC-001-1.1(ii)	R4.	Each Transmission Operator shall coordinate Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.	Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, documentation, electronic logs, computer printouts, or computer demonstration or other equivalent evidence that will be used to confirm that it monitors the Special Protection Systems in its area. (Requirement 6 Part 1)	Each Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1. Each Transmission Operator and Balancing Authority shall keep 90 days of historical data (evidence) for Measures 2 and 3.	Rolling 36 months data retention period.
PRC-001-1.1(ii)	R5.	A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others:	Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, documentation, electronic logs, computer printouts, or computer demonstration or other equivalent evidence that will be used to confirm that it monitors the Special Protection Systems in its area. (Requirement 6 Part 1)	Each Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1. Each Transmission Operator and Balancing Authority shall keep 90 days of historical data (evidence) for Measures 2 and 3.	Rolling 36 months data retention period.
PRC-004-5(i)	R1.	Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: [Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning] 1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and 1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and 1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3,and M4 for a minimum of 12 calendar months following the completion of each Requirement.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		intervention in response to its Protection System failure to operate.			
PRC-004-5(i)	R2.	R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, provide notification as described in Parts 2.1 and 2.2. [Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning] 2.1 For a BES interrupting device operation by a Composite Protection System or by manual intervention in response to a Protection System failure to operate, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances: 2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other owner; and 2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and 2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation. 2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's BES Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2. Acceptable evidence for Requirement R2, including Parts 2.1 and 2.2 may include, but is not limited to the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3, and M4 for a minimum of 12 calendar months following the completion of each Requirement.	Rolling 12 months data retention period.
PRC-004-5(i)	R3.	R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3,	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, identify whether its Protection System component(s) caused a Misoperation. [Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]	System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals. Standard PRC-004-5(i) — Protection System Misoperation Identification and Correction Page 4 of 37	and M4 for a minimum of 12 calendar months following the completion of each Requirement.	
PRC-004-5(i)	R4.	R4. Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3, shall perform investigative action(s) to determine the cause(s) of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: [Violation Risk Factor: High] [Time Horizon: Operations Assessment, Operations Planning] • The identification of the cause(s) of the Misoperation; or • A declaration that no cause was identified.	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it performed at least one investigative action according to Requirement R4 every two full calendar quarters until a cause is identified or a declaration is made. Acceptable evidence for Requirement R4 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals.	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3,and M4 for a minimum of 12 calendar months following the completion of each Requirement.	Rolling 12 months data retention period.
PRC-004-5(i)	R5.	R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [Violation Risk Factor: High] [Time Horizon: Operations Planning, Long-Term Planning] • Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to the following dated documentation (electronic or hardcopy format): CAP and evaluation, or declaration.	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5, including any supporting analysis per Requirements R1, R2, R3, and R4, for a minimum of 12 calendar months following completion of each CAP, completion of each evaluation, and completion of each declaration.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		including other locations; or • Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.			
PRC-004-5(i)	R6.	R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. [Violation Risk Factor: High][Time Horizon: Operations Planning, Long-Term Planning]	Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to the following dated documentation (electronic or hardcopy format): records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.	The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for a minimum of 12 calendar months following completion of each CAP.	Rolling 12 months data retention period.
PRC-005-1.1b	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System that affects the reliability of the BES, shall have an associated Protection System maintenance and testing program as defined in Requirement 1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System, shall retain evidence of the implementation of its Protection System maintenance and testing program for three years. The Compliance Monitor shall retain any audit data for three years.	Rolling 36 Months data retention period.
PRC-005-6	R3.	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-3, and Table 5. [Violation Risk	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included within its time-based program in accordance with Requirement R3. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated	For Requirement R2, Requirement R3, and Requirement R4, in cases where the interval of the maintenance activity is longer than the audit cycle, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component. In cases where the interval of the maintenance activity is shorter than the audit cycle, documentation of all performances (in	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Factor: High] [Time Horizon: Operations Planning]	inspection records, or dated work orders.	accordance with the tables) of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date shall be retained.	
PRC-005-6	R4.	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the performancebased program(s). [Violation Risk Factor: High] [Time Horizon: Operations Planning]	Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the PSMP for the Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included in its performance-based program in accordance with Requirement R4. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.	For Requirement R2, Requirement R3, and Requirement R4, in cases where the interval of the maintenance activity is longer than the audit cycle, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component. In cases where the interval of the maintenance activity is shorter than the audit cycle, documentation of all performances (in accordance with the tables) of that maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date shall be retained.	Rolling 36 months data retention period.
PRC-006-3	R10.	Each Transmission Owner shall provide automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, as determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission. [VRF: High][Time Horizon: Long-term Planning]	Each Transmission Owner shall have dated evidence such as relay settings, tripping logic or other dated documentation that it provided automatic switching of its existing capacitor banks, Transmission Lines, and reactors in order to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for implementation, including any Corrective Action Plan, per Requirement R10.	Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.
PRC-006-3	R15.	Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall develop a Corrective Action Plan and a schedule for	Each Planning Coordinator that conducts a UFLS design assessment under Requirement R4, R5, or R12 and determines that the UFLS program does not meet the performance characteristics in Requirement R3, shall have a dated Corrective Action Plan and a schedule for	Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		implementation by the UFLS entities within its area. [VRF: High][Time Horizon: Long-term Planning]	implementation by the UFLS entities within its area, that was developed within the time frame identified in Part 15.1 or 15.2.		
PRC-006-3	R3.	Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). [VRF: High][Time Horizon: Long-term Planning]	Each Planning Coordinator shall have evidence such as reports, memorandums, e-mails, program plans, or other documentation of its UFLS program, including the notification of the UFLS entities of implementation schedule, that meet the criteria in Requirement R3, Parts 3.1 through 3.3.	Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.
PRC-006-3	R4.	Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2. The simulation shall model each of the following: [VRF: High][Time Horizon: Long-term Planning]	Each Planning Coordinator shall have dated evidence such as reports, dynamic simulation models and results, or other dated documentation of its UFLS design assessment that demonstrates it meets Requirement R4, Parts 4.1 through 4.7.	Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.
PRC-006-3	R5.	Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall coordinate its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island through one of the following: [VRF: High][Time Horizon: Long-term Planning]	Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall have dated evidence such as joint UFLS program design documents, reports describing a joint UFLS design assessment, letters that include recommendations, or other dated documentation demonstrating that it coordinated its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island per Requirement R5.	Transmission Owner shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R10, Measure M10, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
PRC-006-3	R9.	Each UFLS entity shall provide automatic tripping of Load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, as determined by its Planning Coordinator(s) in each Planning Coordinator area in which it owns assets. [VRF: High][Time Horizon: Long-term Planning]	Each UFLS Entity shall have dated evidence such as spreadsheets summarizing feeder load armed with UFLS relays, spreadsheets with UFLS relay settings, or other dated documentation that it provided automatic tripping of load in accordance with the UFLS program design and schedule for implementation, including any Corrective Action Plan, per Requirement R9.	Each UFLS entity shall retain the current evidence of adherence with the UFLS program in accordance with Requirement R9, Measure M9, and evidence of adherence since the last compliance audit.	Rolling 36 months data retention period.
PRC-010-2	R1.	Each Planning Coordinator or Transmission Planner that is developing a UVLS Program shall evaluate its effectiveness and subsequently provide the UVLS Program's specifications and implementation schedule to the UVLS entities responsible for implementing the UVLS Program. The evaluation shall include, but is not limited to, studies and analyses that show: [Violation Risk Factor: High] [Time Horizon: Long-term Planning] 1.1. The implementation of the UVLS Program resolves the identified undervoltage issues that led to its development and design. 1.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, autoreclosing, Remedial Action Schemes, and other undervoltage-based load shedding programs.	Acceptable evidence may include, but is not limited to, date-stamped studies and analyses, reports, or other documentation detailing the effectiveness of the UVLS Program, and date-stamped communications showing that the UVLS Program specifications and implementation schedule were provided to UVLS entities.	The applicable entity shall retain documentation as evidence for six calendar years.	Rolling 36 months data retention period.
PRC-010-2	R2.	Each UVLS entity shall adhere to the UVLS Program specifications and implementation schedule determined by its Planning Coordinator or Transmission Planner associated with UVLS Program development per Requirement R1 or with any Corrective Action Plans per Requirement R5. [Violation Risk Factor: High]	Acceptable evidence must include date-stamped documentation on the completion of actions and may include, but is not limited to, identifying the equipment armed with UVLS relays, the UVLS relay settings, associated Load summaries, work management program records, work orders, and maintenance records.	The applicable entity shall retain documentation as evidence for six calendar years.	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		[Time Horizon: Long-term Planning]			
PRC-017-1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns a RAS shall have a system maintenance and testing program(s) in place. The program(s) shall include: R1.1. RAS identification shall include but is not limited to: R1.1.1. Relays. R1.1.2. Instrument transformers. R1.1.3. Communications systems, where appropriate. R1.1.4. Batteries. R1.2. Documentation of maintenance and testing intervals and their basis. R1.3. Summary of testing procedure. R1.4. Schedule for system testing. R1.5. Schedule for system maintenance. R1.6. Date last tested/maintained.	The Transmission Owner, Generator Owner, and Distribution Provider that owns a RAS shall have a system maintenance and testing program(s) in place that includes all items in Reliability Standard PRC-017-1_R1.	None specified.	Rolling 36 months data retention period.
PRC-023-4	R1.	Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the Set transmission line relays applied at the load center terminal, remote from generation stations, so they do not operate at or below 115% of the maximum current flow from the load to the generation source under any system configuration. Set transmission line relays applied on the bulk system-end of transmission lines that serve load remote to the system so they do not operate at or below 115% of the maximum current flow from the system to the load under any system configuration. Set transmission line relays applied on the load-end of transmission lines that serve load remote to the bulk system so they do not operate at or below 115% of the maximum current flow from the load to the system under any system configuration. Set transformer fault protection relays and transmission line relays on transmission lines terminated only with a transformer so that the relays do not operate at or below the greater of:· 150% of the	Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its transmission relays is set according to one of the criteria in Requirement R1, criterion 1 through 13 and shall have evidence such as coordination curves or summaries of calculations that show that relays set per criterion 10 do not expose the transformer to fault levels and durations beyond those indicated in the standard. (R1)	The Transmission Owner, Generator Owner, and Distribution Provider shall each retain documentation to demonstrate compliance with Requirements R1 through R5 for three calendar years.	Rolling 36 Months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		applicable maximum transformer nameplate rating (expressed in amperes), including the forced cooled ratings corresponding to all installed supplemental cooling equipment.· 115% of the highest operator established emergency transformer rating. Set load-responsive transformer fault protection relays, if used, such that the protection settings do not expose the transformer to a fault level and duration that exceeds the transformer's mechanical withstand capability. For transformer overload protection relays that do not comply with the loadability component of Requirement R1, criterion 10 set the relays according to one of the following:· Set the relays to allow the transformer to be operated at an overload level of at least 150% of the maximum applicable nameplate rating, or 115% of the highest operator established emergency transformer rating, whichever is greater, for at least 15 minutes to provide time for the operator to take controlled action to relieve the overload.· Install supervision for the relays using either a top oil or simulated winding hot spot temperature element set no less than 100° C for the top oil temperature or no less than 140° C for the winding hot spot temperature.12. When the desired transmission line capability is limited by the requirement to adequately protect the transmission line, set the transmission line distance relays to a maximum of 125% of the apparent impedance (at the impedance angle of the transmission line) subject to the following constraints:a. Set the maximum torque angle (MTA) to 90 degrees or the highest supported by the manufacturer.B. Evaluate the relay loadability in amperes at the relay trip point at 0.85 per unit voltage and a power factor angle of 30 degrees.C. Include a relay setting			

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		component of 87% of the current calculated in Requirement R1, criterion 12 in the Facility Rating determination for the circuit. 13. Where other situations present practical limitations on circuit capability, set the phase protection relays so they do not operate at or below 115% of such limitations. 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. [Violation Risk Factor: High] [Time Horizon: Long Term Planning].Criteria:1. Set transmission line relays so they do not operate at or below 150% of the highest seasonal Facility Rating of a circuit, for the available defined loading duration nearest 4 hours (expressed in amperes).2. Set transmission line relays so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating1 of a circuit (expressed in amperes).3. Set transmission			
PRC-023-4	R2.	Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]	Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence such as spreadsheets or summaries of calculations to show that each of its out-of-step blocking elements is set to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1. (R2)	The Transmission Owner, Generator Owner, and Distribution Provider shall each retain documentation to demonstrate compliance with Requirements R1 through R5 for three calendar years.	Rolling 36 Months data retention period.
PRC-023-4	R6.	Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in PRC-023-4, Attachment B to	Each Planning Coordinator shall have evidence such as power flow results, calculation summaries, or study reports that it used the criteria established within PRC-023-4,	The Planning Coordinator shall retain documentation of the most recent review process required in Requirement R6. The Planning Coordinator shall retain the most recent list of circuits in its Planning	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: [Violation Risk Factor: High] [Time Horizon: Long Term Planning] 6.1 Maintain a list of circuits subject to PRC-023-4 per application of Attachment B, including identification of the first calendar year in which any criterion in PRC-023-4, Attachment B applies. 6.2 Provide the list of circuits to all Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within 30 calendar days of the establishment of the initial list and within 30 calendar days of any changes to that list.	Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard as described in Requirement R6. The Planning Coordinator shall have a dated list of such circuits and shall have evidence such as dated correspondence that it provided the list to the Regional Entities, Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area within the required timeframe. (R6)	Coordinator area for which applicable entities must comply with the standard, as determined per Requirement R6.	
PRC-025-2	R1.	Each Generator Owner, Transmission Owner, and Distribution Provider shall apply settings that are in accordance with PRC-025-2 – Attachment 1: Relay Settings, on each load-responsive protective relay while maintaining reliable fault protection. [Violation Risk Factor: High] [Time Horizon: Long-Term Planning]	For each load-responsive protective relay, each Generator Owner, Transmission Owner, and Distribution Provider shall have evidence (e.g., summaries of calculations, spreadsheets, simulation reports, or setting sheets) that settings were applied in accordance with PRC-025-2 – Attachment 1: Relay Settings.	The Generator Owner, Transmission Owner, and Distribution Provider shall retain evidence of Requirement R1 and Measure M1 for the most recent three calendar years.	Rolling 36 Months data retention period.
PRC-026-1	R2.	Each Generator Owner and Transmission Owner shall, once each calendar year, identify each Element for which it applies a load-responsive protective relay at a terminal of an Element that meets either of the following criteria, if any: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Long-term Planning] Criteria: 1. An Element that has tripped since January 1, 2003, due to a power swing during an actual system Disturbance where the Disturbance(s) that caused the trip due to a	Each Generator Owner and Transmission Owner shall have dated evidence that demonstrates the evaluation was performed according to Requirement R2. Evidence may include, but is not limited to, the following documentation: apparent impedance characteristic plots, email, design drawings, facsimiles, R-X plots, software output, records, reports, transmittals, lists, settings sheets, or spreadsheets.	The Generator Owner and Transmission Owner shall retain evidence of Requirement R2 evaluation for a minimum of 12 calendar months following completion of each evaluation where a CAP is not developed.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		power swing continues to be credible. 2. An Element that has formed the boundary of an island since January 1, 2003, during an actual system Disturbance where the Disturbance(s) that caused the islanding condition continues to be credible.			
TOP-001-4	R1.	Each Transmission Operator shall act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions. [Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicableRequirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R2.	Each Balancing Authority shall act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions. [Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R3.	Each Balancing Authority, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Transmission Operator(s), unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicableRequirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			Area via its own actions or by issuing Operating Instructions.	Authority to retain specific evidence for a longer period of time as part of an investigation.	
TOP-001-4	R4.	Each Balancing Authority, Generator Operator, and Distribution Provider shall inform its Transmission Operator of its inability to comply with an Operating Instruction issued by its Transmission Operator. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R5.	Each Transmission Operator, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Balancing Authority, unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicableRequirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R6.	Each Transmission Operator, Generator Operator, and Distribution Provider shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R7.	Each Transmission Operator shall assist other Transmission Operators	Each Transmission Operator shall have and provide evidence which	Each Balancing Authority, Transmission Operator, Generator Operator, and	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		within its Reliability Coordinator Area, if requested and able, provided that the requesting Transmission Operator has implemented its comparable Emergency procedures, unless such assistance cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Distribution Provider shall each keep data or evidence for each applicableRequirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	
TOP-001-4	R8.	Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R10.	Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicableRequirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TOP-001-4	R11.	Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations] 10.1. Monitor Facilities	Each Transmission Operator shall have and provide evidence which may include but is not limited to dated operator logs, dated records, dated and time-stamped voice recordings or dated transcripts of voice recordings, electronic	Each Balancing Authority, Transmission Operator, Generator Operator, and Distribution Provider shall each keep data or evidence for each applicable Requirement R1 through R11, and Measure M1 through M11, for the current calendar year and one previous calendar	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		within its Transmission Operator Area; 10.2. Monitor the status of Remedial Action Schemes within its Transmission Operator Area; 10.3. Monitor non-BES facilities within its Transmission Operator Area identified as necessary by the Transmission Operator; 10.4. Obtain and utilize status, voltages, and flow data for Facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator; 10.5. Obtain and utilize the status of Remedial Action Schemes outside its Transmission Operator Area identified as necessary by the Transmission Operator; and 10.6. Obtain and utilize status, voltages, and flow data for non-BES facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator.	communications, or equivalent documentation, that will be used to determine that it acted to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	
TOP-001-4	R12.	Each Balancing Authority shall monitor its Balancing Authority Area, including the status of Remedial Action Schemes that impact generation or Load, in order to maintain generation-Load-interchange balance within its Balancing Authority Area and support Interconnection frequency. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	Each Transmission Operator shall make available evidence to show that for any occasion in which it operated outside any identified Interconnection Reliability Operating Limit (IROL), the continuous duration did not exceed its associated IROL Tv. Such evidence could include but is not limited to dated computer logs or reports in electronic or hard copy format specifying the date, time, duration, and details of the excursion. If such a situation has not occurred, the Transmission Operator may provide an attestation that an event has not occurred.	Each Transmission Operator shall retain evidence for three calendar years of any occasion in which it has exceeded an identified IROL and its associated IROL Tv as specified in Requirement R12 and Measure M12.	Rolling 36 Months data retention period.
TOP-001-4	R13.	Each Transmission Operator shall keep data or evidence for Requirement R13 and Measure M13 for a rolling 30-day period, 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 have, and make available upon request, evidence to show it ensured that a Real-Time Assessment was performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.	Each Transmission Operator shall keep data or evidence for Requirement R13 and Measure M13 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 30-day data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
TOP-001-4	R14.	Each Transmission Operator shall retain evidence and that it initiated its Operating Plan to mitigate a SOL exceedance as specified in Requirement R14 and Measurement M14 for three calendar years.	Each Transmission Operator shall have evidence that it initiated its Operating Plan for mitigating SOL exceedances identified as part of its Real-time monitoring or Real-time Assessments. This evidence could include but is not limited to dated computer logs showing times the Operating Plan was initiated, dated checklists, or other evidence.	Each Transmission Operator shall retain evidence and that it initiated its Operating Plan to mitigate a SOL exceedance as specified in Requirement R14 and Measurement M14 for three calendar years.	Rolling 36 Months data retention period.
TOP-001-4	R16.	Each Transmission Operator shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Transmission Operator has provided its System Operators with the authority to approve planned outages and maintenance of telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.	Each Transmission Operator and Balancing Authority shall each keep data or evidence for each applicable Requirement R15 through R19, and Measure M15 through M19 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.	Rolling 12 months data retention period.
TOP-001-4	R17.	Each Balancing Authority shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Balancing Authority shall have, and provide upon request, evidence that could include but is not limited to a documented procedure or equivalent evidence that will be used to confirm that the Balancing Authority has provided its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.	Each Transmission Operator and Balancing Authority shall each keep data or evidence for each applicable Requirement R15 through R19, and Measure M15 through M19 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days.	Rolling 12 months data retention period.
TOP-001-4	R18.	Each Transmission Operator shall operate to the most limiting parameter in instances where there is a difference in SOLs. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	Each Transmission Operator shall have, and provide upon request, evidence that could include but is not limited to operator logs, voice recordings, electronic communications, or equivalent evidence that will be used to determine if it operated to the most	Each Transmission Operator and Balancing Authority shall each keep data or evidence for each applicable Requirement R15 through R19, and Measure M15 through M19 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
			limiting parameter in instances where there is a difference in SOLs.	retained for a minimum of 90 calendar days.	
TOP-001-4	R20.	Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	Each Transmission Operator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments as specified in the requirement.	Each Transmission Operator shall keep data or evidence for Requirement R20 and Measure M20 for the current calendar year and one previous calendar year.	Rolling 12 months data retention period.
TOP-001-4	R23.	Each Balancing Authority shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and analysis functions. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	Each Balancing Authority shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, including redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order to perform its Real-time monitoring and analysis functions as specified in the requirement.	Each Balancing Authority shall keep data or evidence for Requirement R23 and Measure M23 for the current calendar year and one previous calendar year.	Rolling 12 months data retention period.
TOP-010-1(i)	R1.	R1. Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include: [Violation Risk Factor: High] [Time Horizon: Real-time Operations]1.1. Criteria for evaluating the quality of	Each Transmission Operator shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in	The applicable entity shall retain evidence of compliance for Requirements R1, R2, and R4, and Measures M1, M2, and M4 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Real-time data;1.2. Provisions to indicate the quality of Real-time data to the System Operator; and1.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.	electronic or hard copy format meeting all provisions of Requirement R1; and 2) evidence the Transmission Operator implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.	longer period of time as part of an investigation.	
TOP-010-1(i)	R2.	Each Balancing Authority shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. The Operating Process or Operating Procedure shall include: [Violation Risk Factor: High] [Time Horizon: Real-time Operations] 2.1. Criteria for evaluating the quality of Real-time data; 2.2. Provisions to indicate the quality of Real-time data to the System Operator; and 2.3. Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects its analysis functions.	Each Balancing Authority shall have evidence that it implemented its Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its analysis functions and Real-time monitoring. This evidence could include, but is not limited to: 1) an Operating Process or Operating Procedure in electronic or hard copy format meeting all provisions of Requirement R2; and 2) evidence the Balancing Authority implemented the Operating Process or Operating Procedure as called for in the Operating Process or Operating Procedure, such as dated operator logs, dated checklists, voice recordings, voice transcripts, or other evidence.	The applicable entity shall retain evidence of compliance for Requirements R1, R2, and R4, and Measures M1, M2, and M4 for the current calendar year and one previous calendar year, with the exception of operator logs and voice recordings which shall be retained for a minimum of 90 calendar days, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.	Rolling 12 months data retention period.
TPL-001-4	R1.	Each Transmission Planner and Planning Coordinator shall maintain System models within its respective area for performing the studies needed to complete its Planning Assessment. The models shall use data consistent with that provided in accordance with the MOD-010 and MOD-012 standards, supplemented by other sources as needed, including items represented in the Corrective Action Plan, and shall represent projected System conditions. This establishes Category P0 as the normal System condition in Table 1. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]	Each Transmission Planner and Planning Coordinator shall provide evidence, in electronic or hard copy format, that it is maintaining System models within their respective area, using data consistent with MOD-010 and MOD-012, including items represented in the Corrective Action Plan, representing projected System conditions, and that the models represent the required information in accordance with Requirement R1.	The models utilized in the current in-force Planning Assessment and one previous Planning Assessment in accordance with Requirement R1 and Measure M1.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
TPL-001-4	R2.	Each Transmission Planner and Planning Coordinator shall prepare an annual Planning Assessment of its portion of the BES. This Planning Assessment shall use current or qualified past studies (as indicated in Requirement R2, Part 2.6), document assumptions, and document summarized results of the steady state analyses, short circuit analyses, and Stability analyses. [Violation Risk Factor: High] [Time Horizon: Long-term Planning]	Each Transmission Planner and Planning Coordinator shall provide dated evidence, such as electronic or hard copies of its annual Planning Assessment, that it has prepared an annual Planning Assessment of its portion of the BES in accordance with Requirement R2.	The Planning Assessments performed since the last compliance audit in accordance with Requirement R2 and Measure M2.	Rolling 36 Months data retention period.
TPL-007-1	R4.	Each responsible entity, as determined in Requirement R1, shall complete a GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon once every 60 calendar months. This GMD Vulnerability Assessment shall use a study or studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. [Violation Risk Factor: High] [Time Horizon: Long-term Planning]	Each responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its GMD Vulnerability Assessment meeting all of the requirements in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its GMD Vulnerability Assessment within 90 calendar days of completion to its Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and to any functional entity who has submitted a written request and has a reliability-related need as specified in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R4.	For Requirement R4, each responsible entity shall retain documentation of the current GMD Vulnerability Assessment and the preceding GMD Vulnerability Assessment.	Current plan, model, agreement, methodology, study, program or procedure with a revision history specifying changes and dates of review.
TPL-007-1	R7.	Responsible entities as determined in Requirement R1that conclude through the GMD Vulnerability	Each responsible entity, as determined in Requirement R1, that concludes, through the GMD Vulnerability	For Requirement R7, each responsible entity shall retain documentation as evidence for five years or until all actions in	Rolling 36 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		Assessment conducted in Requirement R3 that their System does not meet the performance requirements of Table 1 shall develop a Corrective Action Plan addressing how the performance requirements will be met. The Corrective Action Plan shall: [Violation Risk Factor: High] [Time Horizon: Long-term Planning]	Assessment conducted in Requirement R4, that the responsible entity's System does not meet the performance requirements of Table 1 shall have evidence such as electronic or hard copies of its Corrective Action Plan, as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its Corrective Action Plan or relevant information, if any, within 90 calendar days of its completion to its Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), a functional entity referenced in the Corrective Action Plan, and any functional entity that submits a written request and has a reliability-related need, as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its Corrective Action Plan within 90 calendar days of receipt of those comments, in accordance with Requirement R7.	the Corrective Action Plan are completed, whichever is later.	
VAR-001-5	R1.	Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. [Violation Risk Factor: High] [Time Horizon: Operations Planning]1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with	The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of	The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months.	Rolling 12 months data retention period.

Reliability Standard	Req.	Requirement Text	Measure	Data Retention Period Detail	New Evidence Retention Recommendation
		an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.	a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.		
VAR-001-5	R2.	Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. [Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]	Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operations planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.	The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months.	Rolling 12 months data retention period.
VAR-001-5	R3.	Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. [Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]	Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include, but is not limited to, instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.	The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months.	Rolling 12 months data retention period.

Project 2019-04 Modifications to PRC-005-6

Action

Reconsider the action to appoint chair, vice chair, and members with the removal of candidates 1 and 7, to Project 2019-04 Modifications to PRC-005-6 Standard Authorization Request (SAR) drafting team, as approved by the Standards Committee (SC) on November 20, 2019.

Background

From July 30 to August 28, 2019, NERC solicited nominations for a Project 2019-04 Modifications to PRC-005-6 SAR DT. NERC staff received ten nominations and recommended ten individuals with the requisite background, experience, and skills necessary for membership on the SAR DT. On November 20, 2019, the Standards Committee voted to appoint eight (8) of the recommended individuals to the SAR DT. The SC voted to not appoint candidates 1 and 7.

On December 3, 2019 the SC chair, vice chair, and the NERC VP of Engineering and Standards received a request to reconsider appointing candidate 1 to the SAR DT. The email stated:

> [Company] would like to formally request that the NERC Standards Committee reconsider the nominee submission of [candidate #1] to the NERC SDT on PRC-005-6. While we believe that we sufficiently provided the requisite information to have NERC vet this candidate in the prior round of considerations and properly meet the candidacy requirements, [Company] offers the three attached statements of advocation to foster reconsideration of our nominee. These companies have registrations as DP, TO, GO, and or GOP and represent organizations in multiple NERC regions. Lastly, I would have you note that a reference from the original nomination submission is from another multi-registered organization.

Confidential materials will be provided to the SC under separate cover.

For reference, the SC-endorsed *Drafting Team Nominee Selection Criteria* states:

> Members of a DT may include employees or agents of a NERC registered entity or other individuals with expertise related to reliability matters. For all individuals not directly employed by a Registered Entity which are recommended for appointment to a DT, NERC staff shall ensure one of the following criteria is met:

1. As part of the DT member nomination form, a NERC Registered Entity endorses in writing, the individual's participation on the DT as a subject matter expert; or

2. The individual is a subject matter expert on the subject of the development activity.

Standards Committee Guideline

Drafting Team Nominee Selection Criteria

Background: At its December 2017 Standards Committee (SC) Meeting, SC members sought clarification on who could be nominated to a Drafting Team (DT). In determining its recommendation for DT members, NERC seeks to ensure all DT members provide value-added input, provide unbiased subject matter expertise, and promote the reliability of the Bulk Electric System.

Purpose: To provide guidelines for individuals to serve on a DT.

Criteria: Members of a DT may include employees or agents of a NERC registered entity or other individuals with expertise related to reliability matters. For all individuals not directly employed by a Registered Entity which are recommended for appointment to a DT, NERC staff shall ensure one of the following criteria is met:

1. As part of the DT member nomination form, a NERC Registered Entity endorses in writing, the individual's participation on the DT as a subject matter expert[1]; or
2. The individual is a subject matter expert on the subject of the development activity.

Expectations: All Drafting Team members are required to adhere to the *Standard Processes Manual*, *Standards Development Process – Participant Conduct Policy*[2], and *Standards Drafting Team Scope.*

[1] In the event the Registered Entity ends the support/endorsement during the individual's appointment to the drafting team, the individual shall resign from the team.

[2] The *Standards Development Process – Participant Conduct Policy* shall contain the following statement: "Participants shall not use the standards development process for commercial purposes or for their own private purposes, including, but not limited to, advertising or promoting a specific product or service, announcements of a personal nature, sharing of files or attachments not directly relevant to the purpose of the standards development process, and communication of personal views or opinions, unless those views are directly related to the purpose of the standards development process."

Version History

Version	Date	Owner	Change Tracking
1	March 14, 2018	NERC Standards Committee	N/A

Project Management and Oversight Subcommittee

Action
Informational

Background
The Project Management and Oversight Subcommittee (PMOS) leadership appointments have not changed for 2020, therefore, the PMOS did not make an appointment request to the Standards Committee in the third quarter of 2019. Charles Yeung, Southwest Power Pool, continues to serve as chair, and Michael Brytowski, Great Rivers Energy, continues to serve as vice chair. This is consistent with the PMOS Scope with the expectation that officers serve a two-year term with no term limits.

NERC Legal and Regulatory Update

November 8 – December 4, 2019

NERC FILINGS TO FERC SUBMITTED SINCE LAST SC UPDATE

FERC Docket No.	Filing Description	FERC Submittal Date
RM13-11-000	2019 Frequency Response Annual Analysis report NERC submitted its 2019 Frequency Response Annual Analysis report for the administration and support of Reliability Standard BAL-003-1.1 – Frequency Response and Frequency Bias Setting.	11/21/2019

FERC ISSUANCES SINCE LAST SC UPDATE

FERC Docket No.	Issuance Description	FERC Issuance Date
	No FERC Orders since last SC Update	

NERC PLANNED UPCOMING FILINGS

FERC Docket No.	Filing Description	Planned Filing Date
	Reliability Standards Development Plan (RSDP)	12/13/2019
	BAL-003-2 – Frequency Response and Frequency Bias Setting	12/19/2019
	PRC-006-NPCC-2 – Automatic Underfrequency Load Shedding	December 2019
	BAL Informational Filing (Order No. 835 Directive – PP 46 and 58)	December 2019

Standards Committee Executive Committee Election Process

Action

Informational

Background

The following process will be used to elect the three at-large Standards Committee Executive Committee (SCEC) members who will serve on the SCEC for a one-year term:

> No later than the 18th day of December of each year, the Standards Committee (SC) secretary shall solicit (via email) candidates to service in the at-large positions of the SCEC. SC members wishing to self-nominate for one of the at-large SCEC positions must: (i) send an email to the SC secretary expressing interest in running no later than 15 days prior to the January SC meeting date, and (ii) provide a brief, written statement of interest in and qualifications for serving on the SCEC.

The SC secretary shall provide the SC members (via email) the list of nominees and their statements no less than ten days prior to the January SC meeting. The SCEC at-large election, including any run-offs, will take place in the following manner:

> At the start of each January SC meeting, the SC secretary will ask SC members to vote within the first hour of the meeting (via email or other specified electronic means if the meeting is not a face-to-face meeting). If a run-off election becomes necessary, the SC secretary will notify the SC members during the meeting and ask SC members to vote in the run-off election. The SC secretary will announce the results, including vote totals, before the end of the meeting and the names of the winners will be included in the SC meeting minutes.
>
> Each SC member may cast a vote for up to three SCEC nominees. The three nominees with the highest number of votes and a simple majority of the SC members' votes will serve as at-large SCEC members. The SC chair and vice chair have the right to vote in the election. If necessary, run-off elections will take place until three nominees have each received a simple majority of SC members voting.

Pursuant to Section 7 of the SC Charter, the Committee has an Executive Committee consisting of five members, including the Committee officers and three at-large members, elected by the SC. The three at-large members cannot represent the same industry segments as the Committee officers previously represented (Amy Casuscelli, Segment 5 and Todd Bennett, Segment 3), nor can two of the at-large members be from the same segment. The SC will elect the three at-large SCEC members annually at the January SC meeting. The SC used a similar process for previous SCEC elections.

Standards Committee Special Election

Action
Information only.

Background
After the Standards Committee member term election was conducted in late 2019, vacancies remain for the following segments and terms:

- Segment 4, 2020-2021
- Segment 7, 2020-2021
- Segment 9, 2019-2020
- Segment 9, 2020-2021

A Special Election will be conducted to fill these vacancies, with nominations accepted from industry approximately January 24 – February 13, 2020, and election running February 24 – March 4, 2020.

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.

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.