NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee (SC) Meeting

April 16, 2025 | 1:00 – 3:00 p.m. Eastern

Virtual Meeting

Click here to: Register for Webinar

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

Introduction and Chair's Remarks

Agenda Items

1. **Review April 16, 2025 Agenda - Approve -** Todd Bennett*, SC Chair*
2. **Consent Agenda* - Approve -** Todd Bennett*, SC Chair*
   a. March 19, 2025 Standards Committee Meeting Minutes
3. **Project 2020-06 Verifications of Models and Data for Generators* - Approve/Authorize –** Sandhya Madan*, NERC Staff*
   a. Definitions
   b. Implementation Plan
4. **Project 2021-01 System Model Validation with IBRs* - Approve/Authorize –** Sandhya Madan*, NERC Staff*
   a. MOD-033-3
   b. Implementation Plan
5. **Project 2022-02 Uniform Modeling Framework for IBR* - Approve/Authorize –** Sandhya Madan*, NERC Staff*
   a. MOD-032-2
   b. IRO-010-6
   c. TOP-003-8
   d. Implementation Plan
   e. ERO Approved Criteria for Acceptable Models
6. **Errata to Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7, and CIP-011-4* - Approve –** Alison Oswald*, NERC Staff*
   a. CIP-006-7
   b. CIP-007-7

c. CIP-008-7

d. CIP-009-7

e. CIP-011-4

7. **Project 2024-01 Rules of Procedure Definitions Alignment (Generator Owner and Generator Operator)* - Reject -** Alison Oswald*, NERC Staff*

   a. IBR Registration and Standards Applicability Glossary Update Standard Authorization Request

8. **Canadian-Specific Revisions to EOP-012-3 – Extreme Cold Weather Preparedness and Operations* - Accept/Authorize –** Alison Oswald*, NERC Staff*

   a. Canadian-specific Revision to proposed standard EOP-012-3 – Extreme Cold Weather Preparedness and Operations Standard Authorization Request

9. **Update on NERC Board of Trustees Action for Project 2024-03 Revisions to EOP-012-2 - Informational -** Jamie Calderon*, NERC Staff*

10. **Projects Under Review - Review**

    a. Project Tracking Spreadsheet - Mike Brytowski*, PMOS Chair*

    b. Projected Posting Schedule & Three-Month Outlook - Nasheema Santos*, NERC Staff*

11. **Legal Update and Upcoming Standards Filings - Review** - Alain-Christian Rigaud*, NERC Staff*

12. **Informational Items* - Enclosed**

    a. Standards Committee Expectations

    b. 2025 SC Meeting Schedule

    c. 2025 Standards Committee Roster

    d. Highlights of Parliamentary Procedure

13. **Adjournment**

*Background materials included.

Minutes
Standards Committee Meeting

T. Bennett, chair, called to order the meeting of the Standards Committee (SC or the Committee) on March 19, 2025, at 11:04 a.m. Eastern. D. Love determined the meeting had quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement
K. Boyd called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice and directed questions to NERC's General Counsel, Sonia C. Rocha.

Introduction and Chair's Remarks
T. Bennett welcomed the Committee, guests, and proxies to the meeting. T. Bennett informed the Committee that agenda item 13 will move up in the agenda due to a time conflict. S. Kelly provided remarks and provided an update on the Modernization Standards Process and Procedures Task Force. M. Lauby provided remarks and thanked the Committee for their collaboration on the cold weather project.

Review March 19, 2025 Agenda (agenda item 1)
The Committee approved the March 19, 2025, meeting agenda.

Consent Agenda (agenda item 2)
The Committee approved January 22, 2025, Standards Committee Meeting Minutes. T. Bennett appointed Claudine Fritz as the Project Management Oversight Subcommittee Vice Chair.

Quarterly Standards Committee Training (agenda item 3)
S. Crawford provided quarterly training on the Committee elections. S. Bodkin asked about the process of nomination for an election and mentioned that the language in the Rules of Procedure (ROP) does not allow Standards Balloting and Commenting System (SBS) users to nominate. Only Registered Ballot Body (RBB) representatives are allowed to nominate for consideration to participate as a member on the Committee. T. Bennett responded that the language in the ROP pertaining to elections may introduce some ambiguity which could lead to different interpretations. C. Cook recommended that the term SBS be added to the ROP. S. Crawford reiterated that we do not have registered users in the RBB registered, users are in the SBS. The ROP language allows registered users of the SBS system to be eligible for nomination.

Project 2021-01 System Model Validation with IBRs (agenda item 4)
T. Bennett reminded the Committee to refrain from using any identifying information to protect the candidate's identity. S. Madan provided an overview and highlighted that the project is a Milestone 3 project. Committee members expressed their support for the recommendation from NERC staff. P. MacDonald made a motion to appoint five supplemental candidates to the Project 2021-01 System Model Validation with IBRs Drafting Team (DT), as recommended by NERC staff. M. Powell second the motion. S.

Bodkin discussed that the DT is over-represented by the WECC region and proposed amending the motion by replacing candidate 1 with candidate 9. The amendment did not receive a second.

The committee approved the motion with no abstentions. Sean Bodkin opposed.

Project 2020-06 Verifications of Models and Data for Generators (agenda item 5)
S. Madan provided an overview. C. Cook asked the need to supplement the DT. S. Madan responded that the DT experienced issues with meeting quorum and with the additional Standard Authorization Request (SAR), a different set of expertise will be needed to address the new SAR. J. Hale inquired if there were any other options considered in addressing the SAR and if there are any tools that the Committee could do to help support the process. S. Madan responded that there have been milestone workshops to increase engagement and provide transparency in the collaborative efforts among the Milestone 3 projects. The DT believes that they do not have the appropriate skillset to address the objectives in the SAR. T. Pyle asked how NERC is managing the quorum issue on the DT. J. Calderon responded that during the life of the process, unforeseen changes with DT members happens which affects the participation from members. J. Blume mentioned that the DT roster has been reviewed and removed members due to time commitments. T. Bennett asked if the DT leadership set the expectations with DT members about quorum. J. Blume acknowledged the comment and responded that he will take the recommendation back to DT leadership. C. Fritz made a motion to authorize a 30-calendar day solicitation of nominations to supplement the DT. R. Shu (proxy for Dave Krueger) second the motion.

The committee approved the motion with no oppositions and no abstentions.

Project 2022-04 EMT Modeling (agenda item 6)
J. Calderon provided an overview and highlighted that the project is not a milestone 3 project. The DT reviewed the SAR and believed that they did not have the appropriate expertise to address the SAR. Additionally, the DT considered additional nominees but decided that Project 2023-05 would be best suited to handle the SAR. S. Bodkin inquired if NERC considered creating a new DT to address the SAR. J. Calderon responded that project 2023-05 DT has not been seated. There was a discussion about SAR workload on Project 2023-05 and the prioritization of projects. J. Calderon responded that the DT will make the determination of workload once seated and that both projects will retain their current designation of priority. S. Bodkin made a motion to create a new DT to address the Revisions to FAC-001-4 and FAC-002-4 SAR. V. O'Leary second the motion. There were further discussions about multiple projects revising the same standards. FAC-002 revisions made by different projects could be confusing for industry to track.

The motion failed as Jamie Johnson, Patti Metro, Josh Hale, Jennie Wike, Maggy Powell, Venona Greaff, Robert Blohm, Paul MacDonald, and Steven Rueckert opposed with Daniela Cismaru and Ruida Shu (proxy for Dave Krueger) abstained.

T. Bennett recommended that the Committee could delay action on the SAR as this option would allow for additional discussions with the DT. S. Bodkin responded that per Roberts' Rules section 31, the Committee cannot postpone past the next meeting. S. Crawford responded that section 31 of Roberts' Rules was not applicable as it pertained to nominations for elections and that the Committee has the option to postpone

indefinitely. P. MacDonald made a motion to authorize reassignment of Revisions to FAC-001-4 and FAC-002-4 SAR to Project 2023-05 Modifications to FAC-001 and FAC-002 DT. P. Metro second the motion.

The committee approved the motion with no abstentions. Vicki O'Leary, Sean Bodkin, and Maggy Powell opposed.

EOP-012-3 Cold Weather Update (agenda item 13)

T. Bennett provided an update and highlighted the collaborative work amongst the Committee small team and the DT. There were several meetings conducted, both closed and open to the public and a summary was forwarded at the end of the meeting day. At the conclusion of the comment period, there were 125 pages of comments received from industry stakeholders. The small team condensed the comments into themes and incorporated changes into the standard. The standard was currently in Quality Review. A special Board of Trustees (the Board) meeting is scheduled for April 4, 2025. J. Calderon added that due to the significant number of comments, Standards Development asked the Board to hold a special call on April 4, 2025, with an anticipated filing to FERC shortly thereafter. M. Lauby thanked the volunteers and provided support for the recommendation to the Board. An observer asked about filing the standard after the FERC original date of March 27, 2025. J. Calderon responded about the need to have due diligence on industry comments and that an informal action may be pursued to submit after the original deadline. S. Kelly mentioned the importance of the filing to be reflective of the comments received. There was a discussion on the informal extension and why NERC did not consider filing an extension prior to the deadline as industry has been focused on the original FERC filing date. J. Calderon responded that extraordinary circumstances are the reason why NERC has decided to file after the deadline. S. Kelly responded that filing after the deadline is not the optimal action but supports ensuring that stakeholder comments have been adequately addressed in the filing.

Project 2023-08 Modifications of MOD-031 Demand and Energy Data (agenda item 7)

S. Madan provided an update. There was a discussion about the lack of nominations received during the initial solicitation of DT members as one nomination was received. A question was asked about the prioritization of the project. J. Calderon responded that the project is low priority and with the restructuring of prioritization, projects that were on hold will start to resume work. S. Bodkin commented that due to SAR comments and low priority, NERC should consider ending the project. J. Calderon reminded the Committee that this project could be off ramped depending on the criteria developed from the Project Scope Efficiencies group. S. Rueckert made a motion to authorize a 30-day solicitation of nominations to supplement the DT. S. Bodkin second the motion.

The committee approved the motion with no oppositions and no abstentions.

Project 2024-01 Rules of Procedure Definitions Alignment (Generator Owner and Generator Operator) (agenda item 8)

J. Calderon provided an update and highlighted that this project is addressing the ROP definition changes. J. Wike commented that the definitions help support the work of the milestone 3 projects. R. Shu made a motion to authorize initial posting of modified definitions for Generator Owner (GO) and Generator Operator (GOP) and the associated Implementation Plan for a 45-day formal comment period, with ballot

pool formed in the first 30 days, and parallel initial ballots conducted during the last 10 days of the comment period. S. Bodkin second the motion.

The committee approved the motion with no oppositions and no abstentions.

Standing Committee Self-Assessment Results (agenda item 9)
T. Bennett provided an overview and highlighted the key takeaways from the assessment results to include leveraging executive sessions to enhance communication and transparency. S. Bodkin commented that the ROP prohibits executive sessions. T. Bennett responded that the Committee Executive Committee has a standing meeting every month and is allowed. L. Perotti responded that planning meetings do not need to be public and executive and planning meetings are allowed. C. Fritz inquired about Project Management and Oversight Subcommittee representation in the survey. T. Bennett responded that perspective from PMOS leadership was included.

Standards Committee Process Subcommittee Rule 321 Guidance Document (agenda item 10)
T. Brumfield provided an overview. The objective of the guidance document is to carve out a process to help the Committee navigate the Section 321 of the ROP. The team is broken into three groups with each group having a designated role to bring back language to be incorporated into the document. The group focused on post invocation. M. Powell commented that compliance factors are not considered by the DT and NERC staff, however, they are highly significant when entities are voting. S. Kelly mentioned that the Board chair is interested in an effort on lessons learned.

Modernize Standard Processes and Procedures Update (agenda item 11)
J. Calderon provided an overview and highlighted that the Modernize Standard Processes and Procedures (MSPP) recommendations are due to the Board in February 2026. T. Bennett commented that the taskforce is in the early stages of development and all meetings are closed. There was a discussion on the participation of NERC staff in the taskforce and the potential outcomes from the task force. T. Bennett commented that a revision to the Standards Process Manual and front-end concepts approach are being considered. M. Powell commented that the role of compliance and the technical rationale helps support the standards development process.

Standards Development Efficiencies Group Update (agenda item 12)
D. Love provided an overview and highlighted that the group conducted one meeting and discussed meeting cadence and overall goals. The group will bring recommendations for off-ramping projects to the Committee by the end of 2025. S. Bodkin asked if the group meetings are open. D. Love responded that the working meetings will be closed.

Reliable IBR Integration and Milestone 3 of FERC Order No. 901 Update (agenda item 14)
S. Madan provided an update and highlighted that there is another workshop on the horizon and the location will be announced soon.

Projects Under Review (agenda item 15)
M. Brytowski reviewed the Project Tracking Spreadsheet. N. Santos reviewed the Project Posting Schedule and three-month outlook.

Update Legal Update and Upcoming Standards Filings (agenda item 16)
S. Crawford provided an update.

High Priority Project Updates (agenda item 17)
P. Quinn provided an update on Project 2023-06 CIP-014 Risk Assessment Refinement. M. Turner provided an update on Project 2024-02 Planning Energy Assurance.

Subcommittee Updates (agenda item 18)
M. Brytowski provided an update on the Project Management and Oversight Subcommittee. T. Brumfield provided an update on the Standards Committee Process Subcommittee. T. Bennett provided an update on the Standing Committees Coordinating Group. T. Bennett provided an update on the Reliability Issues Steering Committee.

Adjournment
The meeting adjourned at 2:47 p.m. Central.

Standards Committee
2025 Segment Representatives

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Chair 2024-25	Todd Bennett* Managing Director, Reliability Compliance & Audit Services	Associated Electric Cooperative, Inc.		y
Vice Chair 2024-25	Troy Brumfield* Regulatory Compliance Manager	American Transmission Company		y
Segment 1-2024-25	Charlie Cook Lead Compliance Analyst	Duke Energy		y
Segment 1-2025-26	John Martinez Director- Transmission Operations	FirstEnergy		y
Segment 2-2024-25	Jamie Johnson Infrastructure Compliance Manager	California ISO		y
Segment 2-2025-26	N/A	None		n/a
Segment 3-2024-25	Claudine Fritz Principal Compliance Specialist	Exelon Corporation		y
Segment 3-2025-26	Vicki O' Leary Director – Reliability, Compliance, and Implementation	Eversource Energy		y
Segment 4-2024-25	Marty Hostler Reliability Compliance Manager	Northern California Power Agency		n
Segment 4-2025-26	Patti Metro* Senior Grid Operations & Reliability Director	National Rural Electric Cooperative Associate		y
Segment 5-2024-25	Terri Pyle* Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric		y
Segment 5-2025-26	Josh Hale Commercial Services Manager	Southern Power Company		y

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Segment 6-2024-25	Sean Bodkin Senior Counsel	Dominion Energy		y
Segment 6-2025-26	Jennie Wike Compliance Lead	Tacoma Public Utilities		y
Segment 7-2024-25	Maggy Powell Principal Security Industry Specialist, Energy & Utilities	Amazon Web Services		y
Segment 7-2025-26	Venona Greaff* Senior Energy Analyst	Occidental Chemical Corporation		y
Segment 8-2024-25	Robert Blohm[1] Managing Director	Keen Resources Ltd.		y
Segment 8-2025-26	N/A	None		n/a
Segment 9-2024-25	Paul MacDonald[1] Director Reliability Standards, Compliance and Enforcement	New Brunswick Energy and Utilities Board		y
Segment 9-2025-26	Daniela Cismaru General Counsel	Market Surveillance Administrator		y
Segment 10-2024-25	Dave Krueger Senior Program Manager, Operations	SERC Reliability Corporation	Ruida Shu	y
Segment 10-2025-26	Steven Rueckert Director of Standards	WECC		y

[1] Serving as Canadian Representative
*Denotes SC Executive Committee Member

Project 2020-06 Verifications of Models and Data for Generators

Action

- Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2020-06 Verifications of Models and Data for Generators:
    - Initial formal comment and ballot period reduced from 45 calendar days to as few as 25 calendar days, with ballot pools formed in the first 10 calendar days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 calendar days of the comment period. (Sections 4.7, 4.9)
    - Additional formal comment and ballot period (s) reduced from 45 calendar days to as few as 15 calendar days, with ballot(s) conducted during the last 10 calendar days of the comment period. (Sections 4.9 and 4.12)
    - Final ballot period reduced from 10 calendar days to 5 calendar days. (Section 4.9)
- Authorize posting Project 2020-06 Verifications Model and Data for Generators Modeling definitions for an initial 30-calendar day formal comment and ballot period, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Background

The Federal Energy Regulatory Commission (FERC) issued Order No. 901 on October 19, 2023, which included directives on new or modified NERC Reliability Standard projects. FERC Order No. 901 addresses a wide spectrum of reliability risks to the grid from the application of Inverter Based Resources (IBR), including both utility scale and behind-the-meter or distributed energy resources. Within Order No. 901, there are four milestones that include sets of directives to NERC. NERC Standards Development has identified three active projects (2020-06, 2021-01, and 2022-02) that are directly impacted by the associated FERC directives in Order No. 901.

In addition, to assist readers, please see the following additional documents drafted to help keep the NERC Milestone 3 projects organized.

- FERC Order No. 901 - Summary Information of Milestone 3
- FERC Order No. 901 - Summary Graphic of Milestone 3
- Standards Development Mapping of FERC Order 901 Directives and Other Guidance to Standards Development Projects

NERC staff hosted a joint workshop January 15-17, 2025, in Pheonix, AZ. During the workshop NERC staff and drafting team (DT) members reviewed the FERC directives associated with Milestone 3 and talked through concerns of industry prior to the development or modification of each standard(s) with its associated project.

As a Milestone 3 project, Project 2020-06 addresses the FERC directives in Order No. 901 to develop new or modified Reliability Standards for modeling verification and modeling validation

for registered IBRs, unregistered and aggregated IBR, and aggregated distributed energy resources. Additionally, Project 2020-06 proposes definitions for Model Verification and Model Validation to address the need for a uniform understanding of these terms. The proposed revisions would further incorporate the uniform model framework verifications into FAC-002 to ensure a consistent holistic approach for model data sharing is established since commissioning of the IBR. These standards must be filed with FERC by November 4, 2025, in accordance with Order No. 901.

This initial formal comment period and ballot would include two definitions, Model Verification and Model Validation. The DT worked with industry at the engagement workshop to develop these two definitions that will aid in drafting revisions to MOD-026-2 and Project 2021-01 Reliability Standard MOD-033-2 Requirements. The ballot for these definitions will be conducted separately from the Reliability Standard due to the limited timing of the initial draft postings. A quality review of the definitions was performed from January 17 to February 1, 2025, by NERC legal (Alain Rigaud), members of the Milestone 3 DTs, and industry members (Andy Hoke, NREL). Feedback was also received at the Industry Engagement Workshop where industry helped draft these two definitions.

NERC Standard Processes Manual Section 16.0 Waiver provides as follows:

- The Standards Committee (SC) may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
  - In response to a national emergency declared by the United States or Canadian governments that involves the reliability of the Bulk Electric System (BES) or cyber-attack on the BES;
  - Where necessary to meet regulatory deadlines;
  - Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
  - Where the SC determines that a modification to a proposed Reliability Standard or its requirement(s), a modification to a defined term, a modification to an interpretation, or a modification to a variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

Summary

NERC Standards Development has identified three active projects (2020-06, 2021-01, and 2022-02) that are directly impacted by the associated FERC directives in Order No. 901. Project 2020-06 DT leadership and NERC staff request that the SC approve a waiver for certain provisions of the SPM regarding the length of comment periods and ballots in order to meet the November 2025 regulatory deadline for Project 2020-06 as established by FERC.

Project 2020-06 DT leadership and NERC staff recommend that the SC grant the requested waiver under SPM section 16.0 and shorten the initial formal comment and ballot period for all standards and definitions developed under Project 2020-06 from 45 calendar days to as few as 25 calendar days and any additional formal comment and ballot period(s) from 45 calendar days to as few as 15 calendar days. In addition, Project 2020-06 DT leadership and NERC staff recommend shortening the final ballot of all standards and definitions from 10 calendar days to as few as five (5) calendar days.

NERC staff recommends the SC authorize an initial formal comment and ballot period for Project 2020-06 Verifications Model and Data for Generators definitions for a 30-calendar day formal initial ballot, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed definitions for a formal 30-day comment period with an initial ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR)	November 13, 2024
SAR posted for comment	May 23 – June 26, 2024

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
Board adoption	October, 2025

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. The terms proposed below are intended to be used in MOD-026-2 and other modeling-related standards.

Terms:

Model Verification: The process of confirming that model structure and parameter values represent the equipment or facility design and settings by reviewing equipment or facility design and settings documentation.

Model Validation: The process of comparing measurements with simulation results to assess how closely a model's behavior matches the measured behavior.

Version History

Version	Date	Action	Change Tracking
1	TBD	New Model Validation Definition New Model Verification Definition	

Implementation Plan

Project 2020-06 Verifications of Models and Data for Generators Modeling Definitions

Applicable Standard(s)

- None

Requested Retirement(s)

- None

Prerequisite Standard(s)

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

- None

Applicable Entities

- None

New Terms in the NERC Glossary of Terms

This section includes all the newly defined terms used in the NERC Reliability Standards. New definitions listed below become approved when the proposed Reliability Standard MOD-026-2 Verification and Validation of Dynamic Models and Data or MOD-033-3 Steady-State and Dynamic System Model Validation are approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the NERC Glossary of Terms.

Proposed New Definitions:

Model Validation: The process of comparing measurements with simulation results to assess how closely a model's behavior matches the measured behavior.

Model Verification: The process of confirming that model structure and parameter values represent the equipment or facility design and settings by reviewing equipment or facility design and settings documentation.

Background

The NERC Inverter-Based Resource (IBR) Performance Task Force (IRPTF) undertook an effort to perform a comprehensive review of all NERC Reliability Standards to determine if there were any potential gaps or areas of improvement. The IRPTF identified several issues as part of this effort and documented its findings and recommendations in the "IRPTF Review of NERC Reliability Standards White Paper," which was approved in March 2020 by the Operating Committee and the Planning Committee (now part of the

Reliability and Security Technical Committee (RSTC)). Among the findings noted in the white paper, the IRPTF identified issues with MOD-026-1 and MOD-027-1 and recommended that they should either be revised or a new model verification standard should be developed for Inverter-Based resources (IBRs) since these standards stipulate verification methods and practices which do not provide model verification for the majority of the parameters within an Inverter-Based Resource.

In October 2023, FERC issued Order No. 901,[1] which directs the development of new or modified reliability standards, including new requirements for disturbance monitoring, data sharing, post-event performance validation, and correction of IBR performance. In January 2024, NERC submitted a filing to FERC outlining a comprehensive work plan[2] to address the directives within Order No. 901. Within the work plan, NERC identified milestones that must be accomplished. Milestone 3 has three projects that address issues identified in NERC assessments regarding modeling. The projects include 2020-06 Verifications of Models and Data for Generators,[3] 2022-02 Uniform Modeling Framework for IBR,[4] and 2021-01 System Model Validation with IBRs.[5] All Milestone 3 projects must be filed with FERC by November 4, 2025, with full implementation by January 1, 2030, to comply with Order No. 901.

Project 2020-06 addresses the FERC directives in Order No. 901 to develop new or modified Reliability Standards for modeling verification and modeling validation for registered IBRs. Additionally, Project 2020-06 proposes definitions for the terms “Model Verification” and “Model Validation” to address the need for a uniform understanding of these terms.

General Considerations

Multiple standards in development will use the definition(s), and the proposed implementation timeframe is intended to reflect that any one of those standards may be the first to use one or more of the definitions. Additionally, this implementation plan only affects the date that these new definitions will become effective terms in the NERC Glossary of Terms. A separate implementation plan will be developed for MOD-026-2, including requirements that use these proposed definitions.

Effective Date

Where approval by an applicable governmental authority is required, the definitions shall become effective on the first day of the first calendar quarter that is the effective date of the applicable governmental authority’s order approving the definitions, or as otherwise provided for by the applicable governmental authority.

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

[1] Reliability Standards to Address Inverter-Based Resources, Order No.901, 185 FERC ¶ 61,042 (2023); https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20231019-3157&optimized=false

[2] See Informational Filing of the N. Am. Elec. Reliability Corp. Regarding the Development of Reliability Standards Responsive to Order No. 901., Docket No. RM22-12-000 (January 18, 2024).

[3] https://www.nerc.com/pa/Stand/Pages/Project-2020_06-Verifications-of-Models-and-Data-for-Generators.aspx

[4] https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

[5] https://www.nerc.com/pa/Stand/Pages/Project_2021-01_Modifications_to_MOD-025_and_PRC-019.aspx

Project 2021-01 System Model Validation with IBRs

Action

- Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2021-01 System Model Validation with IBRs:
  - Initial formal comment and ballot period reduced from 45 calendar days to as few as 30 calendar days, with ballot pools formed in the first 10 calendar days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 calendar days of the comment period. (Sections 4.7, 4.9)
  - Additional formal comment and ballot period(s) reduced from 45 calendar days to as few as 15 calendar days, with ballot(s) conducted during the last 10 calendar days of the comment period. (Section 4.12)
  - Final ballot period reduced from 10 calendar days to 5 calendar days. (Section 4.9)
- Authorize posting proposed Project 2021-01 System Model Validation with IBRs proposed Reliability Standard MOD-033-3, and its associated Implementation Plan for an initial 30 calendar day formal comment and ballot period, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Background

The Federal Energy Regulatory Commission (FERC) issued Order No. 901 on October 19, 2023, which included directives on new or modified NERC Reliability Standard projects. FERC Order No. 901 addresses a wide spectrum of reliability risks to the grid from the application of Inverter Based Resources (IBR), including both utility scale and behind-the-meter or distributed energy resources. Within the Order, there are four milestones that include sets of directives to NERC. NERC Standards Development has identified three active projects (2020-06, 2021-01, and 2022-02) that are directly impacted by the associated FERC directives in Order No. 901.

In addition, to assist readers, please see the following additional documents drafted to help keep the NERC Milestone 3 projects organized:

- FERC Order No. 901 - Summary Information of Milestone 3
- FERC Order No. 901 - Summary Graphic of Milestone 3
- Standards Development Mapping of FERC Order 901 Directives and Other Guidance to Standards Development Projects

NERC Staff hosted a joint workshop from January 15-17, 2025, in Pheonix, AZ. During the workshop, NERC staff and drafting team members reviewed the FERC directives associated with Milestone 3 and talked through concerns of industry prior to the development or modification of each standard(s) with its associated project.

This one pager addresses Milestone 3 Project 2021-01 and the FERC directives covering the development of Reliability Standards to address concerns "related to IBRs at all stages of interconnection, planning, and operations." (Id. at P 25). Among other things, FERC directed NERC to revise MOD-033 to require System Model Validation against actual system operational behavior during Disturbances.

All new or modified Reliability Standards and associated Implementation Plans addressing Milestone 3 of Order No. 901 must be filed with FERC by November 4, 2025. NERC Project 2021-01 addresses two (2) FERC directives through modifications to MOD-033-3 in addition to the development of the implementation plan.

At the May 15, 2024, meeting, the Standards Committee (SC) accepted the Standards Authorization Request and assigned it to the Project 2021-01 Modifications to MOD-025 and PRC-019 drafting team (DT). This DT changed the name of the project to "Project 2021-01 System Model Validation with IBRs" and thereby addressed the FERC directives by developing draft Reliability Standard MOD-033-3 and its implementation plan.

A Quality Review for MOD-033-3 and its associated implementation plan was conducted from March 14 to March 24, 2025. Comments were received from NERC legal (Alain Rigaud, Lauren Perotti, and Sarah Crawford), NERC engineering (Hasala Dharmawardena), PMOS Representatives (Donovan Crane, WECC), and industry members (Sarah Habriga, AEP; Todd Bennett, AECI; and Sean Bodkin, Dominion Energy).

NERC Standard Processes Manual Section 16.0 Waiver provides as follows:

- The SC may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
  - In response to a national emergency declared by the United States or Canadian governments that involves the reliability of the BES or cyber-attack on the BES;
  - Where necessary to meet regulatory deadlines;
  - Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
  - Where the SC determines that a modification to a proposed Reliability Standard or its requirement(s), a modification to a defined term, a modification to an interpretation, or a modification to a variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

Summary

Project 2021-01 DT leadership and NERC staff request that the SC approve a waiver for certain provisions of the SPM regarding the length of comment periods and ballots in order to meet the November 2025 development deadline for Project 2021-01 as established by FERC.

Project 2021-01 DT leadership and NERC staff recommend the SC shorten the initial formal comment and ballot period for the standard developed under Project 2021-01 from 45 calendar days to as few as 30 calendar days and any additional formal comment and ballot period(s) from 45 calendar days to as few as 15 calendar days. In addition, the Project 2021-01 DT leadership and NERC staff request shortening the final ballot of the standard and implementation plan from 10 calendar days to as few as five (5) calendar days.

NERC Staff recommends the SC authorize initial formal comment and ballot period for Project 2021-01 System Model Validation with IBRs for a 30-calendar day formal initial ballot, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	May 15, 2024
SAR posted for comment	May 23 – June 28, 2024

Anticipated Actions	Date
30-day formal comment period with 10-day ballot	April 17 – May 16, 2025
20-day formal or informal comment period with additional ballot	July – August, 2025
10-day final ballot	September 2025
Board adoption	October 2025

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):

The terms Model Validation and Distributed Energy Resources refer to proposed definitions being developed by Project 2020-06 Verifications of Models and Data for Generators and Project 2022-02 Uniform Framework for IBR, respectively. As of this posting, the proposed definitions of Model Validation and Distributed Energy Resources are:

Model Validation: The process of comparing measurements with simulation results to assess how closely a model's behavior matches the measured behavior.

Distributed Energy Resources: Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

A. Introduction

1. **Title:** **Steady-State and Dynamic System Model Validation**

2. **Number:** **MOD-033-3**

3. **Purpose:** To establish a comprehensive process for system model validation to facilitate achieving and maintaining adequate model accuracy.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Reliability Coordinator

   4.1.3. Transmission Operator

Effective Date: See Implementation Plan for MOD-033-3.

B. Requirements and Measures

R1. Each Planning Coordinator shall implement a documented Model Validation process for its portion of the existing system that includes the following attributes: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Comparison of the power flow simulation performance of the steady state System model[1] to actual System behavior, represented by state estimator case(s) or other Real-time data sources, at least once every 24 calendar months;

1.2. Comparison of the dynamic local event simulation performance of the dynamic System model to actual System behavior, represented by Real-time data sources such as Disturbance data recording(s), at least once every 24 calendar months (using a dynamic local event that occurs within 24 calendar months of the last dynamic local event used in comparison[2]) and completing each comparison within 24 calendar months of the dynamic local event.

1.3. Guidelines to determine unacceptable differences in performance under Parts 1.1 and 1.2; and

1.4. Guidelines to resolve the unacceptable differences in performance identified under Part 1.3.

M1. Acceptable evidence may include, but is not limited to, a copy of the documented Model Validation process and documentation that demonstrates its implementation in accordance with Requirement R1.

R2. Each Reliability Coordinator and Transmission Operator shall, within 30 calendar days of a written request, provide actual System behavior data (or a written response that it does not have the requested data) to any Planning Coordinator performing Model Validation under Requirement R1. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. Acceptable evidence may include, but is not limited to, a copy of the dated communication(s) in accordance with Requirement R2

[1] System models include unregistered Inverter-Based Resources (IBRs) and aggregate Distributed Energy Resources (DERs) when present. The phrase “unregistered IBR” refers to a Bulk-Power System connected IBR that does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.

[2] If no dynamic local event occurs within this 24 calendar months period, use the next dynamic local event that occurs.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" 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 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 with Requirements R1 and R2, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Planning Coordinator implemented a documented Model Validation process but failed to address one of the four attributes stipulated in Requirement R1, Parts 1.1 through 1.4. OR The Planning Coordinator performed the comparison as stipulated in Parts 1.1 or 1.2 but was late by less than or equal to 4 calendar months.	The Planning Coordinator implemented a documented Model Validation process but failed to address two of the four attributes stipulated in Requirement R1, Parts 1.1 through 1.4. OR The Planning Coordinator performed the comparison as stipulated in Parts 1.1 or 1.2 but was late by more than 4 calendar months but less than or equal to 8 calendar months.	The Planning Coordinator implemented a documented Model Validation process but failed to address three of the four attributes stipulated in Requirement R1, Parts 1.1 through 1.4. OR The Planning Coordinator performed the comparison as stipulated in Parts 1.1 or 1.2 but was late by more than 8 calendar months but less than or equal to 12 calendar months.	The Planning Coordinator failed to have a documented Model Validation process in accordance with Requirement R1. OR The Planning Coordinator failed to implement its documented Model Validation process in accordance with Requirement R1. OR The Planning Coordinator performed the comparison as stipulated in Parts 1.1 or 1.2 but was late by more than 12 calendar months.
R2.	The Reliability Coordinator or Transmission Operator provided the requested System behavior data or written response that it does not have the requested data to a requesting Planning Coordinator in accordance with Requirement R2 but	The Reliability Coordinator or Transmission Operator provided the requested System behavior data or written response that it does not have the requested data to a requesting Planning Coordinator in accordance with Requirement R2 but was late by more than 15	The Reliability Coordinator or Transmission Operator provided the requested System behavior data or written response that it does not have the requested data to a requesting Planning Coordinator in accordance with Requirement R2 but was late by more than 30 calendar	The Reliability Coordinator or Transmission Operator provided the requested System behavior data or written response that it does not have the requested data to a requesting Planning Coordinator but was late by more than 45 calendar days. OR The Reliability Coordinator or Transmission Operator failed to provide the requested System

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	was late by less than or equal to 15 calendar days.	calendar days but less than or equal to 30 calendar days.	days but less than or equal to 45 calendar days.	behavior data or written response that it does not have the requested data to a requesting Planning Coordinator.

D. Regional Variances

None.

E. Associated Documents

- MOD-033-3 Implementation Plan
- MOD-033-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees	Developed as a new standard for system validation to address outstanding directives from FERC Order No. 693 and recommendations from several other sources.
1	May 1, 2014	FERC Order issued approving MOD-033-1.	
2	February 6, 2020	Adopted by the NERC Board of Trustees.	Revisions under Project 2017-07
2	October 30, 2020	FERC Order approving MOD- 033-2. Docket No. RD20-4-000	
2	April 1, 2021	Effective Date	
3	TBD	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2021-01

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	May 15, 2024
SAR posted for comment	May 23 – June 28, 2024

Anticipated Actions	Date
30-day formal comment period with 10-day ballot	April 17 – May 16, 2025
20-day formal or informal comment period with additional ballot	July – August, 2025
10-day final ballot	September 2025
Board adoption	October 2025

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):

The terms Model Validation and Distributed Energy Resources refer to proposed definitions being developed by Project 2020-06 Verifications of Models and Data for Generators and Project 2022-02 Uniform Framework for IBR, respectively. As of this posting, the proposed definitions of Model Validation and Distributed Energy Resources are:

Model Validation: The process of comparing measurements with simulation results to assess how closely a model's behavior matches the measured behavior.

Distributed Energy Resources: Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

A. Introduction

1. **Title:** **Steady-State and Dynamic System Model Validation**

2. **Number:** **MOD-033-~~2~~3**

3. **Purpose:** To establish ~~consistent~~a comprehensive process for system model validation ~~requirements~~ to facilitate ~~the collection of accurate data~~achieving and ~~building of planning models to analyze the reliability of the interconnected transmission system~~maintaining adequate model accuracy.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Reliability Coordinator

   4.1.3. Transmission Operator

Effective Date: See Implementation Plan for MOD-033-3

B. Requirements and Measures

R1. Each Planning Coordinator shall implement a documented ~~data validation~~Model Validation process for its portion of the existing system that includes the following attributes: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Comparison of the power flow simulation performance of the ~~Planning Coordinator's portion of the existing system in a planning power flow~~ steady state System model[1] to actual ~~s~~System behavior, represented by ~~a~~ state estimator case(s) or other Real-time data sources, at least once every 24 calendar months ~~through simulation;~~ ;

1.2. Comparison of the dynamic local event simulation performance of the ~~Planning Coordinator's portion of the existing system in a planning dynamic~~dynamic System model to actual ~~system response, through simulation of a dynamic local event,~~System behavior, represented by Real-time data sources such as Disturbance data recording(s), at least once every 24 calendar months (use~~e~~ing a dynamic local event that occurs within 24 calendar months of the last dynamic local event used in comparison~~,~~[2]) and complete~~e~~ing each comparison within 24 calendar months of the dynamic local event.~~). If no dynamic local event occurs within the 24 calendar months, use the next dynamic local event that occurs;~~.

1.3. Guidelines ~~the Planning Coordinator will use~~ to determine unacceptable differences in performance under Parts 1.1 ~~or~~and 1.2; and

1.4. Guidelines to resolve the unacceptable differences in performance identified under Part 1.3.

M1. ~~Each Planning Coordinator shall provide~~Acceptable evidence ~~that it has~~may include, but is not limited to, a copy of the documented ~~validation~~Model Validation process ~~according to Requirement R1 as well as evidence~~and documentation that demonstrates ~~the~~its implementation ~~of the required components of the process~~in accordance with Requirement R1.

R2. Each Reliability Coordinator and Transmission Operator shall, within 30 calendar days of a written request, provide actual ~~s~~System behavior data (or a written response that it does not have the requested data) to any Planning Coordinator performing ~~validation under Requirement R1 within 30 calendar days of a written request, such as, but not limited to, state estimator case or other Real-time data (including disturbance data recordings) necessary for actual system response validation.~~Model

[1] System models include unregistered Inverter-Based Resources (IBRs) and aggregate Distributed Energy Resources (DERs) when present. The phrase "unregistered IBR" refers to a Bulk-Power System connected IBR that does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.

[2] If no dynamic local event occurs within this 24 calendar months period, use the next dynamic local event that occurs.

Validation under Requirement R1. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

~~**M2.** Each Reliability Coordinator and Transmission Operator shall provide evidence, such as email notices or postal receipts showing recipient and date that it has distributed the requested data or written response that it does not have the data, to any Planning Coordinator performing validation under Requirement R1 within 30 days of a written request in accordance with Requirement R2; or a statement by the Reliability Coordinator or Transmission Operator that it has not received notification regarding data necessary for validation by any Planning Coordinator.~~

M2. Acceptable evidence may include, but is not limited to, a copy of the dated communication(s) in accordance with Requirement R2.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" 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~~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 with Requirements R1 ~~through~~ and R2, ~~and Measures M1 through M2,~~ since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

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

~~1.3.~~ Compliance Monitoring and ~~Assessment Processes:~~

~~1.4.~~1.3. ~~Refer to Section 3.0 of Appendix 4C of~~ Enforcement Program: "Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure ~~for~~) or the Commission-approved program of a ~~list of~~Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and ~~assessment processes~~enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

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

~~None~~

~~Table of Compliance Elements~~

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~Long-term Planning~~	~~Medium~~	The Planning Coordinator ~~documented and~~ implemented a documented Model Validation process ~~to validate data~~ but ~~did not~~failed to address one of the four ~~required topics under~~ attributes stipulated in Requirement R1~~;~~, Parts 1.1 through 1.4. OR The Planning Coordinator ~~did not perform simulation~~performed the comparison as ~~required~~stipulated in Parts 1.1 or 1.2 but was late by ~~part 1.1 within 24~~less than or equal to 4 calendar	The Planning Coordinator ~~documented and~~ implemented a documented Model Validation process ~~to validate data~~ but ~~did not~~failed to address two of the four ~~required topics under~~ attributes stipulated in Requirement R1~~;~~, Parts 1.1 through 1.4. OR The Planning Coordinator ~~did not perform simulation~~performed the comparison as ~~required by part 1.1 within 24 calendar months~~ stipulated in Parts 1.1 or 1.2 but ~~did perform the~~	The Planning Coordinator ~~documented and~~ implemented a documented Model Validation process ~~to validate data~~ but ~~did not~~failed to address three of the four ~~required topics under~~ attributes stipulated in Requirement R1~~;~~, Parts 1.1 through 1.4. OR The Planning Coordinator ~~did not perform simulation~~performed the comparison as ~~required by part 1.1 within 24 calendar months~~ stipulated in Parts 1.1 or 1.2 but ~~did perform the~~	The Planning Coordinator ~~did not~~failed to have a ~~validation~~documented Model Validation process ~~at all or did not document or implement any of the four required topics under~~in accordance with Requirement R1~~;~~. OR The Planning Coordinator ~~did not validate~~ failed to implement its ~~portion of the system in the power flow model as required by part 1.1 within 36 calendar months;~~documented Model Validation process in accordance with Requirement R1. OR

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months ~~but did perform the simulation within 28 calendar months;~~ ~~OR~~ ~~The Planning Coordinator did not perform simulation as required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation within 28 calendar months.~~ .	~~simulation in greater~~was late by more than ~~28~~4 calendar months but less than or equal to ~~32~~8 calendar months~~;~~ ~~OR~~ ~~The Planning Coordinator did not perform simulation as required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation in greater than 28 calendar months but less than or equal to 32 calendar months.~~ .	~~simulation in greater~~was late by more than ~~32~~8 calendar months but less than or equal to ~~36 calendar months;~~ ~~OR~~ ~~The Planning Coordinator did not perform simulation as required by part 1.2 within 24 calendar months (or the next dynamic local event in cases where there is more than 24 months between events) but did perform the simulation in greater than 32 calendar months but less than or equal to 36~~12 calendar months.	The Planning Coordinator ~~did not perform simulation as required by part~~ performed the comparison as stipulated in Parts 1.1 or 1.2 ~~within 36 calendar months (or the next dynamic local event in cases where there is~~ but was late by more than ~~24~~12 calendar months ~~between events).~~.

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	~~Long-term Planning~~	~~Lower~~	The Reliability Coordinator or Transmission Operator ~~did not provide~~provided the requested ~~actual system~~System behavior data ~~(~~or ~~a~~ written response that it does not have the requested data~~)~~ to a requesting Planning Coordinator ~~within 30 calendar days of the written request,~~in accordance with Requirement R2 but ~~did provide the data (or written response that it does not have the requested data) in~~ was late by less than or equal to ~~45~~15 calendar days.	The Reliability Coordinator or Transmission Operator ~~did not provide~~provided the requested ~~actual system~~System behavior data ~~(~~or ~~a~~ written response that it does not have the requested data~~)~~ to a requesting Planning Coordinator ~~within 30 calendar days of the written request,~~in accordance with Requirement R2 but ~~did provide the data (or written response that it does not have the requested data) in greater~~was late by more than ~~45~~15 calendar days but less than or equal to ~~60~~30 calendar days.	The Reliability Coordinator or Transmission Operator ~~did not provide~~provided the requested ~~actual system~~System behavior data ~~(~~or ~~a~~ written response that it does not have the requested data~~)~~ to a requesting Planning Coordinator ~~within~~ in accordance with Requirement R2 but was late by more than 30 calendar days ~~of the written request, but did provide the data (or written response that it does not have the requested data) in greater than 60 calendar days~~ but less than or equal to ~~75~~45 calendar days.	The Reliability Coordinator or Transmission Operator ~~did not provide~~provided the requested ~~actual system~~System behavior data ~~(~~or ~~a~~ written response that it does not have the requested data~~)~~ to a requesting Planning Coordinator ~~within 75~~but was late by more than 45 calendar days~~;~~. OR The Reliability Coordinator or Transmission Operator ~~provided a~~failed to provide the requested System behavior data or written response that it does not have the requested data~~, but actually had the data.~~

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to a requesting Planning Coordinator.

D. Regional Variances

None.

~~E. Interpretations~~

~~None.~~

E. Associated Documents

- MOD-033-3 Implementation Plan
- MOD-033-3 Technical Rationale

~~None.~~

~~Guidelines and Technical Basis~~

~~Requirement R1:~~

~~The requirement focuses on the results-based outcome of developing a process for and performing a validation, but does not prescribe a specific method or procedure for the validation outside of the attributes specified in the requirement. For further information on suggested validation procedures, see "Procedures for Validation of Powerflow and Dynamics Cases" produced by the NERC Model Working Group.~~

~~The specific process is left to the judgment of the Planning Coordinator, but the Planning Coordinator is required to develop and include in its process guidelines for evaluating discrepancies between actual system behavior or response and expected system performance for determining whether the discrepancies are unacceptable.~~

~~For the validation in part 1.1, the state estimator case or other Real-time data should be taken as close to system peak as possible. However, other snapshots of the system could be used if deemed to be more appropriate by the Planning Coordinator. While the requirement specifies "once every 24 calendar months," entities are encouraged to perform the comparison on a more frequent basis.~~

~~In performing the comparison required in part 1.1, the Planning Coordinator may consider, among other criteria:~~

1. ~~System load;~~
2. ~~Transmission topology and parameters;~~
3. ~~Voltage at major buses; and~~
4. ~~Flows on major transmission elements.~~

~~The validation in part 1.1 would include consideration of the load distribution and load power factors (as applicable) used in the power flow models. The validation may be made using metered load data if state estimator cases are not available. The comparison of system load distribution and load power factors shall be made on an aggregate company or power flow zone level at a minimum but may also be made on a bus by bus, load pocket (e.g., within a Balancing Authority), or smaller area basis as deemed appropriate by the Planning Coordinator.~~

~~The scope of dynamics model validation is intended to be limited, for purposes of part 1.2, to the Planning Coordinator's planning area, and the intended emphasis under the requirement is on local events or local phenomena, not the whole Interconnection.~~

~~The validation required in part 1.2 may include simulations that are to be compared with actual system data and may include comparisons of:~~

- ~~Voltage oscillations at major buses~~
- ~~System frequency (for events with frequency excursions)~~
- ~~Real and reactive power oscillations on generating units and major inter-area ties~~

~~Determining when a dynamic local event might occur may be unpredictable, and because of the analytic complexities involved in simulation, the time parameters in part 1.2 specify that the comparison period of "at least once every 24 calendar months" is intended to both provide for at least 24 months between dynamic local events used in the comparisons and that comparisons must be completed within 24 months of the date of the dynamic local event used. This clarification ensures that PCs will not face a timing scenario that makes it impossible to comply. If the time referred to the completion time of the comparison, it would be possible for an event to occur in month 23 since the last comparison, leaving only one month to complete the comparison. With the 30 day timeframe in Requirement R2 for TOPs or RCs to provide actual system behavior data (if necessary in the comparison), it would potentially be impossible to complete the comparison within the 24 month timeframe.~~

~~In contrast, the requirement language clarifies that the time frame between dynamic local events used in the comparisons should be within 24 months of each other (or, as specified at the end of part 1.2, in the event more than 24 months passes before the next dynamic local event, the comparison should use the next dynamic local event that occurs). Each comparison must be completed within 24 months of the dynamic local event used. In this manner, the potential problem with a "month 23" dynamic local event described above is resolved. For example, if a PC uses for comparison a dynamic local event occurring on day 1 of month 1, the PC has 24 calendar months from that dynamic local event's occurrence to complete the comparison. If the next dynamic event the PC chooses for comparison occurs in month 23, the PC has 24 months from that dynamic local event's occurrence to complete the comparison.~~

~~Part 1.3 requires the PC to include guidelines in its documented validation process for determining when discrepancies in the comparison of simulation results with actual system results are unacceptable. The PC may develop the guidelines required by parts 1.3 and 1.4 itself, reference other established guidelines, or both. For the power flow comparison, as an example, this could include a guideline the Planning Coordinator will use that flows on 500 kV lines should be within 10% or 100 MW, whichever is larger. It could be different percentages or MW amounts for different voltage levels. Or, as another example, the guideline for voltage comparisons could be that it must be within 1%. But the guidelines the PC includes within its documented validation process should be meaningful for the Planning Coordinator's system. Guidelines for the dynamic event comparison may be less precise. Regardless, the comparison should indicate that the conclusions drawn from the two results should be consistent. For example, the guideline could state that the simulation result will be plotted on the same graph as the actual system response. Then the two plots could be given a visual inspection to see if they look similar or not. Or a guideline could be defined such that~~

~~the rise time of the transient response in the simulation should be within 20% of the rise time of the actual system response. As for the power flow guidelines, the dynamic comparison criteria should be meaningful for the Planning Coordinator's system.~~

~~The guidelines the PC includes in its documented validation process to resolve differences in Part 1.4 could include direct coordination with the data owner, and, if necessary, through the provisions of MOD-032-1, Requirement R3 (i.e., the validation performed under this requirement could identify technical concerns with the data). In other words, while this standard is focused on validation, results of the validation may identify data provided under the modeling data standard that needs to be corrected. If a model with estimated data or a generic model is used for a generator, and the model response does not match the actual response, then the estimated data should be corrected or a more detailed model should be requested from the data provider.~~

~~While the validation is focused on the Planning Coordinator's planning area, the model for the validation should be one that contains a wider area of the Interconnection than the Planning Coordinator's area. If the simulations can be made to match the actual system responses by reasonable changes to the data in the Planning Coordinator's area, then the Planning Coordinator should make those changes in coordination with the data provider. However, for some disturbances, the data in the Planning Coordinator's area may not be what is causing the simulations to not match actual responses. These situations should be reported to the Electric Reliability Organization (ERO). The guidelines the Planning Coordinator includes under Part 1.4 could cover these situations.~~

~~Rationale:During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~In FERC Order No. 693, paragraph 1210, the Commission directed inclusion of "a requirement that the models be validated against actual system responses." Furthermore, the Commission directs in paragraph 1211, "that actual system events be simulated and if the model output is not within the accuracy required, the model shall be modified to achieve the necessary accuracy." Paragraph 1220 similarly directs validation against actual system responses relative to dynamics system models. In FERC Order 890, paragraph 290, the Commission states that "the models should be updated and benchmarked to actual events." Requirement R1 addresses these directives.~~

~~Requirement R1 requires the Planning Coordinator to implement a documented data validation process to validate data in the Planning Coordinator's portion of the existing system in the steady-state and dynamic models to compare performance against~~

~~expected behavior or response, which is consistent with the Commission directives. The validation of the full Interconnection-wide cases is left up to the Electric Reliability Organization (ERO) or its designees, and is not addressed by this standard. The following items were chosen for the validation requirement:~~

~~A. Comparison of performance of the existing system in a planning power flow model to actual system behavior; and~~

~~B. Comparison of the performance of the existing system in a planning dynamics model to actual system response.~~

~~Implementation of these validations will result in more accurate power flow and dynamic models. This, in turn, should result in better correlation between system flows and voltages seen in power flow studies and the actual values seen by system operators during outage conditions. Similar improvements should be expected for dynamics studies, such that the results will more closely match the actual responses of the power system to disturbances.~~

~~Validation of model data is a good utility practice, but it does not easily lend itself to Reliability Standards requirement language. Furthermore, it is challenging to determine specifications for thresholds of disturbances that should be validated and how they are determined. Therefore, this requirement focuses on the Planning Coordinator performing validation pursuant to its process, which must include the attributes listed in parts 1.1 through 1.4, without specifying the details of "how" it must validate, which is necessarily dependent upon facts and circumstances. Other validations are best left to guidance rather than standard requirements.~~

~~Rationale for R2:~~

~~The Planning Coordinator will need actual system behavior data in order to perform the validations required in R1. The Reliability Coordinator or Transmission Operator may have this data. Requirement R2 requires the Reliability Coordinator and Transmission Operator to supply actual system data, if it has the data, to any requesting Planning Coordinator for purposes of model validation under Requirement R1.~~

~~This could also include information the Reliability Coordinator or Transmission Operator has at a field site. For example, if a PMU or DFR is at a generator site and it is recording the disturbance, the Reliability Coordinator or Transmission Operator would typically have that data.~~

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees	Developed as a new standard for system validation to address outstanding directives from FERC Order No. 693 and recommendations from several other sources.
1	May 1, 2014	FERC Order issued approving MOD-033-1.	
2	February 6, 2020	Adopted by the NERC Board of Trustees.	Revisions under Project 2017-07
2	October 30, 2020	FERC Order approving MOD- 033-2. Docket No. RD20-4-000	
2	April 1, 2021	Effective Date	
3	TBD	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2021-01

Implementation Plan

Project 2021-01 System Validation Model with IBRs
Reliability Standard MOD-033-3

Applicable Standard

- MOD-033-3 – Steady-State and Dynamic System Model Validation

Requested Retirement

- MOD-033-2 – Steady-State and Dynamic System Model Validation

Prerequisite Definitions

These definitions must be approved before the Applicable Standard becomes effective:

- Model Validation: The process of comparing measurements with simulation results to assess how closely a model's behavior matches the measured behavior.
- Distributed Energy Resources: Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

Applicable Entities

- Planning Coordinator
- Reliability Coordinator
- Transmission Operator

Background

In October 2023, FERC issued Order No. 901,[1] which directs the development of new or modified reliability standards, including new requirements for disturbance monitoring, data sharing, post-event performance validation, and correction of IBR performance. In January 2024, NERC submitted a filing to FERC outlining a comprehensive work plan[2] to address the directives within Order No. 901. Within the work plan, NERC identified milestones that must be accomplished. Milestone 3 has three projects that address issues identified in NERC assessments regarding modeling. The projects include 2020-06 Verifications of Models and Data for Generators,[3] 2022-02 Uniform Modeling Framework for IBR,[4] and

[1] Reliability Standards to Address Inverter-Based Resources, Order No.901, 185 FERC ¶ 61,042 (2023); https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20231019-3157&optimized=false
[2] See Informational Filing of the N. Am. Elec. Reliability Corp. Regarding the Development of Reliability Standards Responsive to Order No. 901., Docket No. RM22-12-000 (January 18, 2024).
[3] https://www.nerc.com/pa/Stand/Pages/Project-2020_06-Verifications-of-Models-and-Data-for-Generators.aspx
[4] https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

2021-01 System Model Validation with IBRs.[5] All Milestone 3 projects must be filed with FERC by November 4, 2025, with full implementation by January 1, 2030, to comply with Order No. 901.

Project 2021-01 addresses Model Validation of both steady-state and dynamic system models (including registered IBRs, unregistered IBRs and aggregate DERs) against actual system behavior.

General Considerations

MOD-033-3 was developed to address directives issued by the Federal Energy Regulatory Commission (FERC) in Order No. 901 on October 19, 2023. The Order addresses a wide spectrum of reliability risks to the grid from the application of Inverter-Based Resources (IBRs), including both utility scale and behind-the-meter or Distributed Energy Resources (DERs). The modifications to MOD-033 address System Model Validation and complement the work proposed by Project 2020-06 Verifications of Models and Data for Generators and Project 2022-02 Uniform Framework for IBR.

The proposed revisions in MOD-033-3 are intended to improve the clarity of the requirements and are not substantive in nature; i.e., they do not change the scope of the requirements. While MOD-033-3 is not dependent on the proposed revisions to Reliability Standards in the other two Milestone 3 projects, it is dependent on the two proposed Glossary terms "Model Validation" and "Distributed Energy Resources".

This implementation plan is not intended to affect the timelines provided in the implementation plans for the other Milestone 3 Reliability Standards addressing the provision of unregistered IBR data or aggregate DER data.

Effective Date

Where approval by an applicable governmental authority is required, Reliability Standard MOD-033-3 shall become effective on the first day of the first calendar quarter after the effective date of the applicable governmental authority's order approving the standard or order approving the proposed definitions of Model Validation and Distributed Energy Resources, whichever date is later, 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 after the date the standard or the proposed definitions of Model Validation and Distributed Energy Resources are adopted by the NERC Board of Trustees, whichever date is later, or as otherwise provided for in that jurisdiction.

Retirement Date

Reliability Standard MOD-033-2 shall be retired immediately prior to the effective date of Reliability Standard MOD-033-3 in the particular jurisdiction in which the revised standard is becoming effective.

[5] https://www.nerc.com/pa/Stand/Pages/Project_2021-01_Modifications_to_MOD-025_and_PRC-019.aspx

Project 2022-02 Uniform Modeling Framework for IBR

Action

- Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2022-02 Uniform Modeling Framework for IBR:
  - Initial formal comment and ballot period reduced from 45 calendar days to as few as 30 calendar days, with ballot pools formed in the first 10 calendar days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 calendar days of the comment period. (Sections 4.7, 4.9)
  - Additional formal comment and ballot period (s) reduced from 45 calendar days to as few as 15 calendar days, with ballot(s) conducted during the last 10 calendar days of the comment period. (Section 4.12)
  - Final ballot period reduced from 10 calendar days to 5 calendar days. (Section 4.9)
- Authorize posting Project 2022-02 Uniform Modeling Framework for IBR proposed Reliability Standards MOD-032-2, IRO-010-5, TOP-003-8, and the associated Implementation Plan for an initial 30 calendar day formal comment and ballot period, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Background

The Federal Energy Regulatory Commission (FERC) issued Order No. 901 on October 19, 2023, which included directives on new or modified NERC Reliability Standard projects.[1] FERC Order No. 901 addresses a wide spectrum of reliability risks to the grid from the application of Inverter-Based Resources (IBRs), including both utility scale and behind-the-meter or distributed energy resources. Within Order No. 901, there are four milestones that include sets of directives to NERC. NERC Standards Development has identified three active projects (2020-06, 2021-01, and 2022-02) that are directly impacted by the associated FERC directives in Order No. 901.

In addition, to assist readers, please see the following additional documents drafted to help keep the NERC Milestone 3 projects organized.

- FERC Order No. 901 - Summary Information of Milestone 3
- FERC Order No. 901 - Summary Graphic of Milestone 3
- Standards Development Mapping of FERC Order 901 Directives and Other Guidance to Standards Development Projects

This one pager addresses Milestone 3 Project 2022-02 and the FERC directive covering the development of Reliability Standards to address concerns "related to IBRs at all stages of interconnection, planning, and operations.[2]" Among other things, FERC directed NERC to develop

[1] *Reliability Standards to Address Inverter-Based Resources,* Order No. 901, 185 FERC ¶ 61,042 (2023), available at eLibrary | File List.

[2] FERC Order No. 901 at P 25.

requirements addressing the provision of IBR and Distributed Energy Resource (DER) data to the entities responsible for the planning and operation of the Bulk-Power System.

All new or modified Reliability Standards and associated Implementation Plans addressing Milestone 3 of Order No. 901 must be filed with FERC by November 4, 2025. NERC Project 2022-02 addresses 24 FERC directives through modifications to MOD-032-2, IRO-010-5, and TOP-003-8 in addition to the development of the Implementation Plan.

At its November 13, 2024, meeting, the Standards Committee (SC) accepted the FERC Order No. 901 – Milestone 3, Part 1: Modeling and Data Sharing Requirements Standards Authorization Request and appointed this SAR to the 2022-02 Uniform Modeling Framework for IBR DT, as recommended by NERC staff.

NERC staff hosted a joint workshop from January 15-17, 2025, in Pheonix, AZ. During the workshop NERC staff and drafting team (DT) members reviewed the FERC directives associated with Milestone 3 and talked through concerns of industry prior to the development or modification of each standard(s) with its associated project.

A quality review for MOD-032-2, IRO-010-5, and TOP-003-8 and the associated Implementation Plan was conducted from March 14 to March 24, 2025, by NERC legal and engineering (Alain Rigaud, Lauren Perotti, Sarah Crawford, and JP Skeath), members of the DT (Hari Singh, CORE Electric Cooperative), PMOS Representatives (Donovan Crane, WECC), and industry members (Sarah Habriga, AEP; Todd Bennett, AECI; Ruth Kloecker, ITC Holdings; and Sean Bodkin, Dominion Energy).

NERC Standard Processes Manual Section 16.0 Waiver provides as follows:

- The SC may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
    - In response to a national emergency declared by the United States or Canadian governments that involves the reliability of the BES or cyber-attack on the BES;
    - Where necessary to meet regulatory deadlines;
    - Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
    - Where the SC determines that a modification to a proposed Reliability Standard or its requirement(s), a modification to a defined term, a modification to an interpretation, or a modification to a variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

Summary

Project 2022-02 DT leadership and NERC staff request that the SC approve a waiver under section 16.0 of the SPM regarding the length of comment periods and ballots in order to meet the November 2025 regulatory deadline for Project 2022-02 as established by FERC.

Project 2022-02 DT leadership and NERC staff recommend that the SC shorten the initial formal comment and ballot period for all standards and definitions developed under Project 2022-02 from 45 calendar days to as few as 30 calendar days and any additional formal comment and

ballot period(s) from 45 calendar days to as few as 15 calendar days. In addition, Project 2022-02 DT leadership and NERC staff recommend shortening the final ballot of all standards and definitions from 10 calendar days to as few as five (5) calendar days.

NERC staff recommends the SC authorize initial formal comment and ballot period for Project 2022-02 Uniform Modeling Framework for IBR for a 30-calendar day formal initial ballot, with ballot pools formed in the first 10 calendar days, and initial ballots conducted during the last 10 calendar days of the comment period.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	January 19, 2022
SAR posted for comment	February 1 – March 2, 2022
45-day formal comment period with ballot	May 31, 2023 – July 14, 2023
45-day formal comment period with additional ballot	October 6 – November 20, 2023
45-day formal comment period with additional ballot	August 27 – October 10, 2024

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

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):

Distributed Energy Resources (DER): Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

A. Introduction

1. **Title:** **Data for Power System Modeling and Analysis**

2. **Number:** **MOD-032-2**

3. **Purpose:** To establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider

   4.1.3 Generator Owner

   4.1.4 Planning Authority and Planning Coordinator (hereafter collectively referred to as “Planning Coordinator”)

   4.1.5 Resource Planner

   4.1.6 Transmission Owner

   4.1.7 Transmission Planner

   4.1.8 Transmission Service Provider

5. **Effective Date:** See Implementation Plan for Project 2022-02.

B. Requirements and Measures

R1. Each Planning Coordinator and each of its Transmission Planners shall jointly develop steady-state, dynamics, and short circuit modeling data requirements and reporting procedures for the Planning Coordinator's planning area that include: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The data listed in Attachment 1, including the responsible entity for each required item.

1.2. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization (ERO).

1.3. Specifications of the following items consistent with procedures for building the Interconnection-wide case(s):

1.3.1. Data format;

1.3.2. Level of detail to which equipment shall be modeled;

1.3.3. Case types or scenarios to be modeled; and

1.3.4. A schedule for submission of data at least once every 13 calendar months.

1.4. Specifications for distribution or posting of the data requirements and reporting procedures so that they are available to those entities responsible for providing the data.

M1. Each Planning Coordinator and Transmission Planner shall provide evidence that it has jointly developed the required modeling data requirements and reporting procedures specified in Requirement R1.

R2. Each Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, and Transmission Service Provider shall provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1. For data that has not changed since the last submission, a written confirmation that the data has not changed is sufficient. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Energy Resource (DER) data, the responsible entity shall estimate the modeling

2.1. If the responsible entity, as identified in Requirement R1 Part 1.1, is unable to gather unregistered Inverter-based Resource (IBR)[1] data or aggregate Distributed data and parameters and include an explanation of the limitations of the availability of data, an explanation of the limitations of any data provided, and the method used for estimation.

M2. Each registered entity identified in Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted the required modeling data to its Transmission Planner(s) and Planning Coordinator(s); or written confirmation that the data has not changed.

R3. Upon receipt of written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2, including the technical basis or reason for the technical concerns, each notified Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider shall respond to the notifying Planning Coordinator or Transmission Planner as follows: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. Provide either updated data or an explanation with a technical basis for maintaining the current data;

3.2. Provide the response within 90 calendar days of receipt, unless a longer time period is agreed upon by the notifying Planning Coordinator or Transmission Planner.

M3. Each registered entity identified in Requirement R3 that has received written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has provided either updated data or an explanation with a technical basis for maintaining the current data to its Planning Coordinator or Transmission Planner within 90 calendar days of receipt (or within the longer time period agreed upon by the notifying Planning Coordinator or Transmission Planner), or a statement that it has not received written notification regarding technical concerns with the data submitted.

R4. Each Planning Coordinator shall make available models for its planning area reflecting data provided to it under Requirement R2 to the Electric Reliability Organization (ERO) or its designee to support creation of the Interconnection-wide case(s) that includes

[1] As used in this standard, the phrase “unregistered IBR” refers to a Bulk-Power System connected IBR that does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.

the Planning Coordinator's planning area. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted models for its planning area reflecting data provided to it under Requirement R2 when requested by the ERO or its designee.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" 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 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 directive by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

   - Requirements R1 through R4, and Measures M1 through M4, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

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

2. **Compliance Monitoring and Enforcement Program:** Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include less than or equal to 25% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 25%, but less than or equal to 50% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 50%, but less than or equal to 75% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) did not develop any steady-state, dynamics, and short circuit modeling data requirements and reporting procedures required by Requirement R1; OR The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 75% of the required components specified in Requirement R1.
R2	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider did not provide any steady-state, dynamics, and

	steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide less than or equal to 25% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but less than or equal to 25% of the required data failed to meet data format, shareability, level of detail, or case type specifications;	short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 25%, but less than or equal to 50% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 25%, but less than or equal to 50% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource	circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 50%, but less than or equal to 75% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 50%, but less than or equal to 75% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service	short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s); OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 75% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 75% of the required data failed to meet

	OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in less than or equal to 15 calendar days after the specified date.	Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 15, but less than or equal to 30 calendar days after the specified date.	Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 30, but less than or equal to 45 calendar days after the specified date.	data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 45 calendar days after the specified date.
R3	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s)	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s)	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s)

	or Planning Coordinator(s) according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within 105 calendar days (or within 15 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	Coordinator(s) according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 105 calendar days, but less than or equal to 120 calendar days (or within greater than 15 calendar days, but less than or equal to 30 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 120 calendar days, but less than or equal to 135 calendar days (or within greater than 30 calendar days, but less than or equal to 45 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	according to the specifications of Requirement R3 within 135 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).
R4	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide less than or equal to 25% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 25%, but less than or equal to 50% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 50%, but less than or equal to 75% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 75% of the required data in the format specified by the ERO or its designee.

D. Regional Variances

None.

E. Associated Documents

- Project 2022-02 Implementation Plan
- Project 2022-02 Technical Rationale

MOD-032-2 – ATTACHMENT 1
Data Reporting Requirements

The table below indicates the information[1] that is required to effectively model the interconnected transmission system for the Near-Term Transmission Planning Horizon and Long-Term Transmission Planning Horizon. Data must be shareable on an interconnection-wide basis to support use in Interconnection-wide cases. A Planning Coordinator may specify additional information that includes specific information required for each item in the table below. Each functional entity[2] typically responsible for reporting the respective data in the table is identified by brackets "[functional entity]" adjacent to and following each data item. The joint Planning Coordinator /Transmission Planner modeling data requirements and reporting procedures developed under Requirement R1 will specify the functional entity responsibility and data flow processes. The data reported shall be identified by the bus number, name, and/or identifier that is assigned in conjunction with the Planning Coordinator, Transmission Owner, or Transmission Planner.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics**	**short circuit**
1. Each bus [TO] a. nominal voltage b. area, zone and owner 2. Aggregate Demand[3] [DP] a. real and reactive power* b. in-service status* 3. Generating and storage units[4] [GO, TO[5], RP (for future planned resources only)] a. real power capabilities - gross maximum and minimum values b. reactive power capabilities - maximum and minimum values at real power capabilities in 3a above c. station service auxiliary load for normal plant configuration (provide data in the same manner as that required for aggregate Demand under item 2, above).	1. Generator [GO, RP (for future planned resources only)] 2. Excitation System [GO, RP (for future planned resources only)] 3. Governor [GO, RP (for future planned resources only)] 4. Power System Stabilizer [GO, RP (for future planned resources only)] 5. Aggregate Demand[3] [DP] 6. Wind plant model (for plants with type 1 and type 2 wind turbines) [GO] 7. Inverter-Based Resource [GO, TO[5]] a. IBR capabilities related to momentary cessation, tripping, Ride-through, and frequency control 8. Static Var Systems and FACTS [GO, TO, DP] 9. DC system models [TO]	1. Provide for all applicable elements in column "steady-state" [GO, RP, TO, DP] a. Positive Sequence Data b. Negative Sequence Data c. Zero Sequence Data 2. Mutual Line Impedance Data [TO] 3. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics**	**short circuit**
d. regulated bus* and voltage set point* (as typically provided by the TOP) e. machine MVA base f. generator step up transformer data (provide same data as that required for transformer under item 6, below) g. generator type (hydro, wind, fossil, solar, nuclear, etc.) h. in-service status* 4. AC Transmission Line or Circuit [TO] a. impedance parameters (positive sequence) b. susceptance (line charging) c. ratings (normal and emergency)* d. in-service status* 5. DC Transmission systems [TO] 6. Transformer (voltage and phase-shifting) [TO] a. nominal voltages of windings b. impedance(s) c. tap ratios (voltage or phase angle)* d. minimum and maximum tap position limits e. number of tap positions (for both the ULTC and NLTC) f. regulated bus (for voltage regulating transformers)* g. ratings (normal and emergency)* h. in-service status* 7. Reactive compensation (shunt capacitors and reactors) [TO] a. admittances (MVars) of each capacitor and reactor b. regulated voltage band limits* (if mode of operation not fixed) c. mode of operation (fixed, discrete, continuous, etc.) d. regulated bus* (if mode of operation not fixed) e. in-service status* 8. Static Var Systems [TO] a. reactive limits b. voltage set point* c. fixed/switched shunt, if applicable	10. Aggregate Distributed Energy Resource (DER) data [DP, TO][6] a. DER capabilities related to momentary cessation, tripping, Ride-through, voltage control, and frequency control or information that can be used to infer those capabilities for modeling purposes. b. indication whether DER is subject to tripping in conjunction with UFLS or UVLS. 11. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]	

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics**	**short circuit**
d. in-service status* 9. Aggregate Distributed Energy Resource (DER) data [DP, TO][6] a. Location (bus from item 1) b. Real power capability c. DER type (solar, battery, diesel generator, etc.) 10. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]		

Attachment 1 Data Reporting Requirements Footnotes

1. Data specified in the sub-bullets of each column that are required for both steady-state and dynamics are not duplicated in the table.
2. For purposes of this attachment, the functional entity references are represented by abbreviations as follows: Balancing Authority (BA), Distribution Provider (DP), Generator Owner (GO), Planning Coordinator (PC), Resource Planner (RP), Transmission Owner (TO), Transmission Planner (TP), and Transmission Service Provider (TSP).
3. For purposes of this item, aggregate Demand is the gross Demand aggregated at each bus under item 1 under Steady State Column that is identified by a Transmission Owner as a load serving bus rather than the net Demand that incorporates offsets due to output from Distributed Energy Resources. A Distribution Provider is the typical responsible entity for providing this information, generally through coordination with the Transmission Owner.
4. This includes IBR, synchronous condensers, and pumped storage.
5. The Transmission Owner is the typical responsible entity for collecting and providing data for unregistered IBRs that are not DERs.
6. The Distribution Provider is the typical responsible entity for collecting and providing data for DER connected to its system either directly or through an unregistered Distribution Provider (i.e., not included on the NERC Compliance Registry) with no other registered entity systems between the DER connection point and the Distribution Provider’s system. The Transmission Owner is the typical responsible entity for collecting and providing data for DER where there is no associated registered Distribution Provider between the DER connection point and the Transmission Owner’s system.

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees.	Developed to consolidate and replace MOD-010-0, MOD -011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1
1	May 1, 2014	FERC Order issued approving MOD-032-1.	See Implementation Plan posted on the Reliability Standards web page for details on enforcement dates for Requirements.
2	TBD	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2022-02.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	January 19, 2022
SAR posted for comment	February 1 – March 2, 2022
45-day formal comment period with ballot	May 31, 2023 – July 14, 2023
45-day formal comment period with additional ballot	October 6 – November 20, 2023
45-day formal comment period with additional ballot	August 27 – October 10, 2024

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

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):

Distributed Energy Resources (DER): Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

A. Introduction

1. **Title:** **Data for Power System Modeling and Analysis**

2. **Number:** **MOD-032-12**

3. **Purpose:** To establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider

   4.1.24.1.3 Generator Owner

   4.1.3 Load Serving Entity

   4.1.4 Planning Authority and Planning Coordinator (hereafter collectively referred to as "Planning Coordinator")

   This proposed standard combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria list "Planning Authority," and they are not yet synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator.

   4.1.5 Resource Planner

   4.1.6 Transmission Owner

   4.1.7 Transmission Planner

   4.1.8 Transmission Service Provider

5. **Effective Date:** See Implementation Plan for Project 2022-02.

   MOD-032-1, Requirement R1 shall become effective on the first day of the first calendar quarter that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, MOD-032-1, Requirement R1 shall become effective on the first day of the first calendar quarter that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

   MOD-032-1, Requirements R2, R3, and R4 shall become effective on the first day of the first calendar quarter that is 24 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a

jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, MOD-032-1, Requirements R2, R3, and R4 shall become effective on the first day of the first calendar quarter that is 24 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

6. Background:

MOD-032-1 exists in conjunction with MOD-033-1, both of which are related to system-level modeling and validation. Reliability Standard MOD-032-1 is a consolidation and replacement of existing MOD-010-0, MOD-011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1, and it requires data submission by applicable data owners to their respective Transmission Planners and Planning Coordinators to support the Interconnection-wide case building process in their Interconnection. Reliability Standard MOD-033-1 is a new standard, and it requires each Planning Coordinator to implement a documented process to perform model validation within its planning area.

The transition and focus of responsibility upon the Planning Coordinator function in both standards are driven by several recommendations and FERC directives from FERC Order No. 693, which are discussed in greater detail in the rationale sections of the standards. One of the most recent and significant set of recommendations came from the NERC Planning Committee's System Analysis and Modeling Subcommittee (SAMS). SAMS proposed several improvements to the modeling data standards, to include consolidation of the standards (the SAMS whitepaper is available from the December 2012 NERC Planning Committee's agenda package, item 3.4, beginning on page 99, here: http://www.nerc.com/comm/PC/Agendas%20Highlights%20and%20Minutes%20DL/2012/2012_Dec_PC%20Agenda.pdf).

B. Requirements and Measures

R1. Each Planning Coordinator and each of its Transmission Planners shall jointly develop steady-state, dynamics, and short circuit modeling data requirements and reporting procedures for the Planning Coordinator's planning area that include: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The data listed in Attachment 1~~.~~, including the responsible entity for each required item.

1.2. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization (ERO).

~~**1.2.**~~**1.3.** Specifications of the following items consistent with procedures for building the Interconnection-wide case(s):

~~**1.2.1.**~~**1.3.1.** Data format;

~~**1.2.2.**~~**1.3.2.** Level of detail to which equipment shall be modeled;

~~**1.2.3.**~~**1.3.3.** Case types or scenarios to be modeled; and

~~**1.2.4.**~~**1.3.4.** A schedule for submission of data at least once every 13 calendar months.

~~**1.3.**~~**1.4.** Specifications for distribution or posting of the data requirements and reporting procedures so that they are available to those entities responsible for providing the data.

M1. Each Planning Coordinator and Transmission Planner shall provide evidence that it has jointly developed the required modeling data requirements and reporting procedures specified in Requirement R1.

R2. Each Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, and Transmission Service Provider shall provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1. For data that has not changed since the last submission, a written confirmation that the data has not changed is sufficient. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. If the responsible entity, as identified in Requirement R1 Part 1.1, is unable to gather unregistered Inverter-based Resource (IBR)[1] data or aggregate Distributed Energy Resource (DER) data, the responsible entity shall estimate the modeling data and parameters and include an explanation of the limitations of

[1] As used in this standard, the phrase "unregistered IBR" refers to a Bulk-Power System connected IBR that does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.

the availability of data, an explanation of the limitations of any data provided, and the method used for estimation.

M2. Each registered entity identified in Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted the required modeling data to its Transmission Planner(s) and Planning Coordinator(s); or written confirmation that the data has not changed.

R3. Upon receipt of written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2, including the technical basis or reason for the technical concerns, each notified Balancing Authority, Distribution Provider, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider shall respond to the notifying Planning Coordinator or Transmission Planner as follows: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. Provide either updated data or an explanation with a technical basis for maintaining the current data;

3.2. Provide the response within 90 calendar days of receipt, unless a longer time period is agreed upon by the notifying Planning Coordinator or Transmission Planner.

M3. Each registered entity identified in Requirement R3 that has received written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has provided either updated data or an explanation with a technical basis for maintaining the current data to its Planning Coordinator or Transmission Planner within 90 calendar days of receipt (or within the longer time period agreed upon by the notifying Planning Coordinator or Transmission Planner), or a statement that it has not received written notification regarding technical concerns with the data submitted.

R4. Each Planning Coordinator shall make available models for its planning area reflecting data provided to it under Requirement R2 to the Electric Reliability Organization (ERO) or its designee to support creation of the Interconnection-wide case(s) that includes the Planning Coordinator's planning area. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. Each Planning Coordinator shall provide evidence, such as email records or postal receipts showing recipient and date, that it has submitted models for its planning area reflecting data provided to it under Requirement R2 when requested by the ERO or its designee.

C. Compliance

1. **Compliance Enforcement Authority**

   1.1. "Compliance Enforcement Authority" 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 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 directive by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation. ~~with~~

   - Requirements R1 through R4, and Measures M1 through M4, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

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

2. **Compliance Monitoring and Assessment Processes:** Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.~~.~~

~~1.3.~~

~~Refer to the NERC Rules of Procedure for a list of compliance monitoring and assessment processes.~~

~~1.4. Additional Compliance Information~~

~~None~~

~~Table of Compliance Elements~~

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Long-term Planning~~	~~Lower~~	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include less than or equal to 25% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 25%, but less than or equal to 50% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 50%, but less than or equal to 75% of the required components specified in Requirement R1.	The Planning Coordinator and Transmission Planner(s) ~~Coordinator~~ did not develop any steady-state, dynamics, and short circuit modeling data requirements and reporting procedures required by Requirement R1; OR The Planning Coordinator and Transmission Planner(s) developed steady-state, dynamics, and short circuit modeling data requirements and reporting procedures, but failed to include greater than 75% of

						the required components specified in Requirement R1.
R2	~~Long-term Planning~~	~~Medium~~	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide less than or equal to 25% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 25%, but less than or equal to 50% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving~~	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 50%, but less than or equal to 75% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving~~	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider did not provide any steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s); OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided

			Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but less than or equal to 25% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data	~~Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 25%, but less than or equal to 50% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state,	~~Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 50%, but less than or equal to 75% of the required data failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide steady-state,	steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but failed to provide greater than 75% of the required data specified in Attachment 1; OR The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider provided steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s), but greater than 75% of the required data

			to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in less than or equal to 15 calendar days after the specified date.	dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 15, but less than or equal to 30 calendar days after the specified date.	dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 30, but less than or equal to 45 calendar days after the specified date.	failed to meet data format, shareability, level of detail, or case type specifications; OR The Balancing Authority, Distribution Provider, Generator Owner, ~~Load Serving Entity,~~ Resource Planner, Transmission Owner or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 45 calendar days after the specified date.

R3	~~Long-term Planning~~	~~Lower~~	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement ~~R4~~R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within 105 calendar days (or within 15 calendar days after the longer period agreed upon by the notifying Planning Coordinator	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement ~~R4~~R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 105 calendar days, but less than or equal to 120 calendar days (or within greater than 15 calendar days, but less	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement ~~R4~~R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the response within greater than 120 calendar days, but less than or equal to 135 calendar days (or within greater than 30 calendar days, but less	The Balancing Authority, Distribution Provider, Generator Owner~~, Load Serving Entity~~, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement ~~R4~~R3 within 135 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).

			or Transmission Planner).	than or equal to 30 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	than or equal to 45 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	
R4	~~**Long-term Planning**~~	~~**Medium**~~	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide less than or equal to 25% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 25%, but less than or equal to 50% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 50%, but less than or equal to 75% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 75% of the required data in the format specified by the ERO or its designee.

D. Regional Variances

None.

~~E. Interpretations~~

~~None.~~

~~F.~~E. Associated Documents

~~None.~~

- Project 2022-02 Implementation Plan
- Project 2022-02 Technical Rationale

MOD-032-012 – ATTACHMENT 1:

Data Reporting Requirements

The table, below, indicates the information[1] that is required to effectively model the interconnected transmission system for the Near-Term Transmission Planning Horizon and Long-Term Transmission Planning Horizon. Data must be shareable on an interconnection-wide basis to support use in *the* Interconnection-wide cases. A Planning Coordinator may specify additional information that includes specific information required for each item in the table below. Each functional *entity*[2] typically responsible for reporting the respective data in the table is identified by brackets "[functional entity]" adjacent to and following each data item. The joint Planning Coordinator /Transmission Planner modeling data requirements and reporting procedures developed under Requirement R1 will specify the functional entity responsibility and data flow processes. The data reported shall be *as* identified by the bus number, name, and/or identifier that is assigned in conjunction with the *PC, TO*Planning Coordinator, Transmission Owner, or Transmission Planner*TP*.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics** *(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)*	**short circuit**
1. Each bus [TO] a. nominal voltage b. area, zone and owner 2. Aggregate Demand[2] [LSEDemand[3] [DP] a. real and reactive power*	1. Generator [GO, RP (for future planned resources only)] 2. Excitation System [GO, RP (for future planned resources only)]	1. Provide for all applicable elements in column "steady-state" [GO, RP, TO, DP] a. Positive Sequence Data b. Negative Sequence Data c. Zero Sequence Data

[2] For purposes of this item, aggregate Demand is the Demand aggregated at each bus under item 1 that is identified by a Transmission Owner as a load serving bus. A Load Serving Entity is responsible for providing this information, generally through coordination with the Transmission Owner.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. -Those items may have different data provided for different modeling scenarios)*	dynamics *(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)*	short circuit
b. in-service status* 3. Generating Units[3]and storage units[4] [GO, TO[5], RP (for future planned resources only)] a. real power capabilities - gross maximum and minimum values b. reactive power capabilities - maximum and minimum values at real power capabilities in 3a above c. station service auxiliary load for normal plant configuration (provide data in the same manner as that required for aggregate Demand under item 2, above). d. regulated bus* and voltage set point* (as typically provided by the TOP) e. machine MVA base f. generator step up transformer data (provide same data as that required for transformer under item 6, below) g. generator type (hydro, wind, fossil, solar, nuclear, etc.) h. in-service status* h. 4. AC Transmission Line or Circuit [TO] a. impedance parameters (positive sequence) b. susceptance (line charging) c. ratings (normal and emergency)* d. in-service status*	3. Governor [GO, RP (for future planned resources only)] 4. Power System Stabilizer [GO, RP (for future planned resources only)] 5. Demand [LSE]Aggregate Demand[3] [DP] 6. Wind Turbine Dataplant model (for plants with type 1 and type 2 wind turbines) [GO] 7. Photovoltaic systems [GO] 7. Inverter-Based Resource [GO, TO[5]] a. IBR capabilities related to momentary cessation, tripping, Ride-through, and frequency control 8. Static Var Systems and FACTS [GO, TO, LSEDP] 9. DC system models [TO] 10. Aggregate Distributed Energy Resource (DER) data [DP, TO][6] a. DER capabilities related to momentary cessation, tripping, Ride-through, voltage control, and frequency control or information that can be used to infer those capabilities for modeling purposes. b. indication whether DER is subject to tripping in conjunction with UFLS or UVLS. 10.11. Other information requested by the Planning Coordinator or Transmission Planner	2. Mutual Line Impedance Data- [TO] 3. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, LSEDP, TO, TSP]

[3] Including synchronous condensers and pumped storage.

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. -Those items may have different data provided for different modeling scenarios)*	dynamics *~~(If a user-written model(s) is submitted in place of a generic or library model, it must include the characteristics of the model, including block diagrams, values and names for all model parameters, and a list of all state variables)~~*	short circuit
5. DC Transmission systems [TO] 6. Transformer (voltage and phase-shifting) [TO] a. nominal voltages of windings b. impedance(s) c. tap ratios (voltage or phase angle)* d. minimum and maximum tap position limits e. number of tap positions (for both the ULTC and NLTC) f. regulated bus (for voltage regulating transformers)* g. ratings (normal and emergency)* h. in-service status* 7. Reactive compensation (shunt capacitors and reactors) [TO] a. admittances (MVars) of each capacitor and reactor b. regulated voltage band limits* (if mode of operation not fixed) c. mode of operation (fixed, discrete, continuous, etc.) d. regulated bus* (if mode of operation not fixed) e. in-service status* 8. Static Var Systems -[TO] a. reactive limits b. voltage set point* c. fixed/switched shunt, if applicable d. in-service status* 9. Aggregate Distributed Energy Resource (DER) data [DP, TO][6] a. Location (bus from item 1) b. Real power capability c. DER type (solar, battery, diesel generator, etc.) ~~9.~~10. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, ~~LSE~~DP, TO, TSP]	necessary for modeling purposes. [BA, GO, ~~LSE~~DP, TO, TSP]	

Guidelines and Technical Basis

For purposes of jointly developing steady-state, dynamics, and short circuit modeling data requirements and reporting procedures under Requirement R1, if a Transmission Planner (TP) and Planning Coordinator (PC) mutually agree, a TP may collect and aggregate some or all data from providing entities, and the TP may then provide that data directly to the PC(s) on behalf of the providing entities. The submitting entities are responsible for getting the data to both the TP and the PC, but nothing precludes them from arriving at mutual agreements for them to provide it to the TP, who then provides it to the PC. Such agreement does not relieve the submitting entity from responsibility under the standard, nor does it make the consolidating entity liable for the submitting entities' compliance under the standard (in essence, nothing precludes parties from agreeing to consolidate or act as a conduit to pass the data, and it is in fact encouraged in certain circumstances, but the requirement is aimed at the act of submitting the data). Notably, there is no requirement for the TP to provide data to the PC. The intent, in part, is to address potential concerns from entities that they would otherwise be responsible for the quality, nature, and sufficiency of the data provided by other entities.

The requirement in Part 1.3 to include specifications for distribution or posting of the data requirements and reporting procedures could be accomplished in many ways, to include posting on a Web site, distributing directly, or through other methods that the Planning Coordinator and each of its Transmission Planners develop.

An entity submitting data per the requirements of this standard who needs to determine the PC for the area, as a starting point, should contact the local Transmission Owner (TO) for information on the TO's PC. Typically, the PC will be the same for both the local TO and those entities connected to the TO's system. If this is not the case, the local TO's PC can typically provide contact information on other PCs in the area. If the entity (e.g., a Generator Owner [GO]) is requesting connection of a new generator, the entity can determine who the PC is for that area at the time a generator connection request is submitted. Often the TO and PC are the same entity, or the TO can provide information on contacting the PC. The entity should specify as the reason for the request to the TO that the entity needs to provide data to the PC according to this standard. Nothing in the proposed requirement language of this standard is intended to preclude coordination between entities such that one entity, serving only as a conduit, provides the other entity's data to the PC. This can be accomplished if it is mutually agreeable by, for example, the GO (or other entity), TP, and the PC. This does not, however, relieve the original entity from its obligations under the standard to provide data, nor does it pass on the compliance obligation of the entity. The original entity is still accountable for making sure that the data has been provided to the PC according to the requirements of this standard.

The standard language recognizes that differences exist among the Interconnections. Presently, the Eastern/Quebec and Texas Interconnections build seasonal cases on an annual basis, while the Western Interconnection builds cases on a continuous basis throughout the year. The intent of the standard is not to change established processes and procedures in each of the Interconnections, but to create a framework to support both what is already in place or what it may transition into in the future, and

~~to provide further guidance in a common platform for the collection of data that is necessary for the building of the Interconnection-wide case(s).~~

~~The construct that these standards replace did not specifically list which Functional Entities were required to provide specific data. Attachment 1 specifically identifies the entities responsible for the data required for the building of the Interconnection-wide case(s).~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~This requirement consolidates the concepts from the original data requirements from MOD-011-0, Requirement R1, and MOD-013-0, Requirement R1. The original requirements specified types of steady-state and dynamics data necessary to model and analyze the steady-state conditions and dynamic behavior or response within each Interconnection. The original requirements, however, did not account for the collection of short circuit data also required to perform short circuit studies. The addition of short circuit data also addresses the outstanding directive from FERC Order No. 890, paragraph 290.~~

~~In developing a performance-based standard that would address the data requirements and reporting procedures for model data, it was prohibitively difficult to account for all of the detailed technical concerns associated with the preparation and submittal of model data given that many of these concerns are dependent upon evolving industry modeling needs and software vendor terminology and product capabilities.~~

~~This requirement establishes the Planning Coordinator jointly with its Transmission Planners as the developers of technical model data requirements and reporting procedures to be followed by the data owners in the Planning Coordinator's planning area. FERC Order No. 693, paragraphs 1155 and 1162, also direct that the standard apply to Planning Coordinators. The inclusion of Transmission Planners in the applicability section is intended to ensure that the Transmission Planners are able to participate jointly in the development of the data requirements and reporting procedures.~~

~~This requirement is also consistent with the recommendations from the NERC System Analysis and Modeling Subcommittee (SAMS) White Paper titled "Proposed Improvements for NERC MOD Standards", available from the December 2012 NERC Planning Committee's agenda package, item 3.4, beginning on page 99, here:~~

Aside from recommendations in support of strengthening and improving MOD-010 through MOD-015, the SAMS paper included the following suggested improvements:

1) reduce the quantity of MOD standards;
2) add short circuit data as a requirement to the MOD standards; and
3) supply data and models:
    a. add requirement identifying who provides and who receives data;
    b. identify acceptability;
    c. standard format;
    d. how to deal with new technologies (user written models if no standard model exists); and
    e. shareability.
4) These suggested improvements are addressed by combining the existing standards into two new standards, one standard for the submission and collection of data, and one for the validation of the planning models. Adding the requirement for the submittal of short circuit data is also an improvement from the existing standards, consistent with FERC Order No. 890, paragraph 290. In supplying data, the approach clearly identifies what data is required and which Functional Entity is required to provide the data.
5) The requirement uses an attachment approach to support data collection. The attachment specifically lists the entities that are required to provide each type of data and the steady-state, dynamics, and short circuit data that is required.
6) Finally, the decision to combine steady-state, dynamics, and short circuit data requirements into one requirement rather than three reflects that they all support the requirement of submission of data in general.

Rationale for R2:

This requirement satisfies the directive from FERC Order No. 693, paragraph 1155, which directs that "the planning authority should be included in this Reliability Standard because the planning authority is the entity responsible for the coordination and integration of transmission facilities and resource plans, as well as one of the entities responsible for the integrity and consistency of the data."

Rationale for R3:

In order to maintain a certain level of accuracy in the representation of a power system, the data that is submitted must be correct, periodically checked, and updated. Data used to perform steady-state, dynamics, and short circuit studies can change, for example, as a result of new planned transmission construction (in comparison to as-built information) or changes performed during the

~~restoration of the transmission network due to weather-related events. One set of data that changes on a more frequent basis is load data, and updates to load data are needed when new improved forecasts are created.~~

~~This requirement provides a mechanism for the Planning Coordinator and Transmission Planner (that does not exist in the current standards) to collect corrected data from the entities that have the data. It provides a feedback loop to address technical concerns related to the data when the Planning Coordinator or Transmission Planner identifies technical concerns, such as concerns about the usability of data or simply that the data is not in the correct format and cannot be used. The requirement also establishes a time-frame for response to address timeliness.~~

~~Rationale for R4:~~

~~This requirement will replace MOD-014 and MOD-015.~~

~~This requirement recognizes the differences among Interconnections in model building processes, and it creates an obligation for Planning Coordinators to make available data for its planning area.~~

~~The requirement creates a clear expectation that Planning Coordinators will make available data that they collect under Requirement R2 in support of their respective Interconnection-wide case(s). While different entities in each Interconnection create the Interconnection-wide case(s), the requirement to submit the data to the "ERO or its designee" supports a framework whereby NERC, in collaboration and agreement with those other organizations, can designate the appropriate organizations in each Interconnection to build the specific Interconnection-wide case(s). It does not prescribe a specific group or process to build the larger Interconnection-wide case(s), but only requires the Planning Coordinators to make available data in support of their creation, consistent with the SAMS Proposed Improvements to NERC MOD Standards (at page 3) that, "industry best practices and existing processes should be considered in the development of requirements, *as many entities are successfully coordinating their efforts.*" (Emphasis added).~~

~~This requirement is about the Planning Coordinator's obligation to make information available for use in the Interconnection-wide case(s); it is not a requirement to build the Interconnection-wide case(s).~~

~~For example, under current practice, the Eastern Interconnection Reliability Assessment Group (ERAG) builds the Eastern Interconnection and Quebec Interconnection-wide cases, the Western Electricity Coordinating Council (WECC) builds the Western Interconnection-wide cases, and the Electric Reliability Council of Texas (ERCOT) builds the Texas Interconnection-wide cases. This requirement does not require a change to that construct, and, assuming continued agreement by those organizations, ERAG, WECC, and ERCOT could be the "designee" for each Interconnection contemplated by this requirement. Similarly, the requirement does not prohibit transition, and the requirement remains for the Planning Coordinators to make available the information to the ERO or~~

~~to whomever the ERO has coordinated with and designated as the recipient of such information for purposes of creation of each of the Interconnection–wide cases.~~

Attachment 1 Data Reporting Requirements Footnotes

1. Data specified in the sub-bullets of each column that are required for both steady-state and dynamics are not duplicated in the table.
2. For purposes of this attachment, the functional entity references are represented by abbreviations as follows: Balancing Authority (BA), Distribution Provider (DP), Generator Owner (GO), Planning Coordinator (PC), Resource Planner (RP), Transmission Owner (TO), Transmission Planner (TP), and Transmission Service Provider (TSP).
3. For purposes of this item, aggregate Demand is the gross Demand aggregated at each bus under item 1 under Steady State Column that is identified by a Transmission Owner as a load serving bus rather than the net Demand that incorporates offsets due to output from Distributed Energy Resources. A Distribution Provider is the typical responsible entity for providing this information, generally through coordination with the Transmission Owner.
4. This includes IBR, synchronous condensers, and pumped storage.
5. The Transmission Owner is the typical responsible entity for collecting and providing data for unregistered IBRs that are not DERs.
6. The Distribution Provider is the typical responsible entity for collecting and providing data for DER connected to its system either directly or through an unregistered Distribution Provider (i.e., not included on the NERC Compliance Registry) with no other registered entity systems between the DER connection point and the Distribution Provider's system. The Transmission Owner is the typical responsible entity for collecting and providing data for DER where there is no associated registered Distribution Provider between the DER connection point and the Transmission Owner's system.

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees.	Developed to consolidate and replace MOD-010-0, MOD -011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1
1	May 1, 2014	FERC Order issued approving MOD-032-1.	See Implementation Plan posted on the Reliability Standards web page for details on enforcement dates for Requirements.
2	TBD	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2022-02.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	November 13, 2024
SAR posted for comment	May 5 – June 6, 2024
45-day formal comment period with initial ballot	April 17 – May 2, 2025

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

A. Introduction

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

2. **Number:** IRO-010-6

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

4. **Applicability:**

   4.1. Reliability Coordinator

   4.2. Balancing Authority

   4.3. Generator Owner

   4.4. Generator Operator

   4.5. Transmission Operator

   4.6. Transmission Owner

   4.7. Distribution Provider

5. **Effective Date:** See Implementation Plan for Project 2022-02.

B. Requirements

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

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments including non-BES data and information, external network data and information, Inverter-based Resource (IBR)-specific data and parameters, and identification of the entities responsible for responding to the specification as deemed necessary by the Reliability Coordinator.

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

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1 Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints.

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide data and information that includes, but is not limited to:

1.5.1 Specific deadlines or periodicity in which data and information is to be provided;

1.5.2 Performance criteria for the availability and accuracy of data and information, as applicable;

1.5.3 Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization;

1.5.4 Provisions to update or correct data and information, as applicable or necessary;

1.5.5 A mutually agreeable format; and

1.5.6 A mutually agreeable method(s) for securely transferring data and information.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification(s) for data and information.

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

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

- The Reliability Coordinator shall retain its dated, current, in force documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.
- The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.
- Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

1.3. Compliance Monitoring and Enforcement Program:
"Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the DT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet one of the parts in Requirement Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet two of the parts in Requirement R1Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet any of the parts in Requirement R1 Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 did not satisfy the obligations of the documented specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Project 2022-02 Implementation Plan
- Project 2022-02 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO- 010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-3. Docket No. RD20-4-000	
4	March 22, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06 Cold Weather
4	June 11, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	August 24,2021	FERC approved IRO-010-4. Docket No. RD21-5-000	
4	August 27, 2021	Effective Date	April 1, 2023
5	August 17, 2023	Adopted by NERC Board of Trustees	Revision under project 2021-06
5	November 2, 2023	FERC approved IRO-010-5. Docket No. RD23-6-000	
6	TBD	Adopted by the NERC Board of Trustees	Revisions to address FERC Order No. 901 directives.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	November 13, 2024
SAR posted for comment	May 5 – June 6, 2024
45-day formal comment period with initial ballot	April 17 – May 2, 2025

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

A. Introduction

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

2. **Number:** IRO-010-~~5~~6

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

4. **Applicability:**

   4.1. Reliability Coordinator

   4.2. Balancing Authority

   4.3. Generator Owner

   4.4. Generator Operator

   4.5. Transmission Operator

   4.6. Transmission Owner

   4.7. Distribution Provider

5. **Effective Date:** See Implementation Plan for Project ~~2021-06.~~2022-02.

B. Requirements

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

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments including non-BES data and information, external network data and information, Inverter-based Resource (IBR)-specific data and parameters, and identification of the entities responsible for responding to the specification as deemed necessary by the Reliability Coordinator.

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

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1 Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints.

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide data and information that includes, but is not limited to~~.~~:

1.5.1 Specific deadlines or periodicity in which data and information is to be provided;

1.5.2 Performance criteria for the availability and accuracy of data and information, as applicable;

1.5.3 Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization;

~~**1.5.3**~~**1.5.4** Provisions to update or correct data and information, as applicable or necessary~~.~~;

~~1.5.4~~1.5.5 A mutually agreeable format~~.~~; and

~~1.5.5~~1.5.6 A mutually agreeable method(s) for securely transferring data and information.

M1. The Reliability Coordinator shall make available its dated, current, in force documented specification(s) for data and information.

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

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

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~CEA~~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 Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The Reliability Coordinator shall retain its dated, current, in force documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R1, Measure M1 as well as any documents in force since the last compliance audit.
- The Reliability Coordinator shall keep evidence for three calendar years that it has distributed its ~~-~~specification(s) to entities that have data required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments for Requirement R2, Measure M2.
- Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a ~~-~~specification(s) shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R3 and Measurement M3.

1.3. Compliance Monitoring and Enforcement Program:
~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Enforcement Program" ~~refers~~or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the ~~identification~~NERC Rules of Procedure) or the Commission-approved program of ~~the processes~~a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that ~~will be used to evaluate data or information~~is responsible for ~~the purpose of assessing performance or~~

~~outcomes~~performing compliance monitoring and enforcement activities with ~~the associated reliability standard~~respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R1	Operations Planning	Low	The Reliability Coordinator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real- time Assessments.	The Reliability Coordinator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Reliability Coordinator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
For the Requirement R2 VSLs only, the intent of the ~~SDT~~DT is to start with the Severe VSL first and then to work your way to the left until you find the situation that fits. In this manner, the VSL will not be discriminatory by size of entity. If a small entity has just one affected reliability entity to inform, the intent is that that situation would be a Severe violation.						

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower	Moderate	High	Severe
R2	Operations Planning	Low	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to one entity, or 5% or less of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to two entities, or more than 5% and less than or equal to 10% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, and Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to three entities, or more than 10% and less than or equal to 15% of the reliability entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Reliability Coordinator did not distribute its specification(s) as developed in Requirement R1 to four or more entities, or more than 15% of the entities, whichever is greater, that have data and information required by the Reliability Coordinator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R3	Operations Planning, Same-Day Operations, Real-time Operations	Medium	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet one of the parts in Requirement Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet two of the parts in Requirement R1Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 satisfied the obligations of the documented specifications but failed to meet any of the parts in Requirement R1 Part 1.5.	The responsible entity receiving a specification(s) in Requirement R2 did not satisfy the obligations of the documented specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Project 2022-02 Implementation Plan
- Project 2022-002 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	Order issued by FERC approving IRO- 010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	April 2014	Revisions pursuant to Project 2014-03	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC approved IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC approved IRO-010-3. Docket No. RD20-4-000	
4	March 22, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06 Cold Weather
4	June 11, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	August 24,2021	FERC approved IRO-010-4. Docket No. RD21-5-000	
4	August 27, 2021	Effective Date	April 1, 2023
5	August 17, 2023	Adopted by NERC Board of Trustees	Revision under project 2021-06
5	November 2, 2023	FERC approved IRO-010-5. Docket No. RD23-6-000	
6	TBD	Adopted by NERC Board of Trustees	FERC order 901 Modifications

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	November 13, 2024
SAR posted for comment	May 17 – June 24, 2024

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

A. Introduction

1. **Title:** Transmission Operator and Balancing Authority Data and Information Specification and Collection
2. **Number:** TOP-003-8
3. **Purpose:** To ensure that each Transmission Operator and Balancing Authority has the data and information it needs to plan, monitor, and assess the operation of its Transmission Operator Area or Balancing Authority Area.
4. **Applicability:**
   - **4.1** Functional Entities:
     - **4.1.1** Transmission Operator
     - **4.1.2** Balancing Authority
     - **4.1.3** Generator Owner
     - **4.1.4** Generator Operator
     - **4.1.5** Transmission Owner
     - **4.1.6** Distribution Provider
5. **Effective Date:** See Implementation Plan for Project 2022-02.

B. Requirements and Measures

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

1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and information, external network data and information, Inverter-based Resource (IBR)-specific data and parameters, and identification of the entities responsible for responding to the specification as deemed necessary by the Transmission Operator.

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

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1. Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide the data and information that includes, at a minimum, the following:

1.5.1. Specified deadlines or periodicity in which data and information is to be provided;

1.5.2. Performance criteria for the availability and accuracy of data and information as applicable;

1.5.3. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization ;

1.5.4. Provisions to update or correct data and information, as applicable or necessary;

1.5.5. A mutually agreeable format;

1.5.6. Mutually agreeable method(s) for securely transferring data and information.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification(s) for data and information.

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

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments, including non-Bulk Electric System data and information, IBR-specific data and parameters, and external network data and information, as deemed necessary by the Balancing Authority, and identification of the entity responsible for responding to the specification.

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

2.3. Provisions for notification of BES generating unit(s) status during local forecasted cold weather to include:

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s) minimum:

2.3.2.1. design temperature; or

2.3.2.2. historical operating temperature; or

2.3.2.3. current cold weather performance temperature determined by an engineering analysis.

2.4. Identification of a mutually agreeable process in resolving conflicts;

2.5. Methods for the entity identified in Part 2.1 to provide data and information that includes at a minimum the following:

2.5.1. Specific deadlines or periodicity in which data and information is to be provided;

2.5.2. Performance criteria for the availability and accuracy of data and

information, as applicable;

2.5.3. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the ERO;

2.5.4. Provisions to update or correct data and information, as applicable or necessary.

2.5.5. A mutually agreeable format.

2.5.6. A mutually agreeable method(s) for securely transferring data and information.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification(s) for data and information.

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

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification(s) to entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

Such evidence could include, but is not limited to, web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or email records.

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

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

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

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations

of the documented specification. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

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

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

- Each Transmission Operator shall retain its dated, current, in force, documented specification for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.
- Each Balancing Authority shall retain its dated, current, in force, documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R2 and Measurement M2, as well as any documents in force since the last compliance audit.
- Each Transmission Operator shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.
- Each Balancing Authority shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Balancing Authority's analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R4 and Measurement M4.
- Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of

the documented specifications in accordance with Requirement R5 and Measurement M5.

1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R#	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Transmission Operator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R2	The Balancing Authority did not include two or fewer of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include any of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments. OR, The Balancing Authority did not have a documented specification(s) for the data and information necessary for it to perform its analysis functions,

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

R#	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Energy Reliability Assessments.	monitoring, and Near-Term Energy Reliability Assessments.	Assessments.	
R5	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet one of the parts in Requirement R1 Part1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet two of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet three or more of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 did not satisfy the obligations of the documented specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- 2022-02 Implementation Plan
- 2022-02 Technical Rationale

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP- 003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
4	October 30, 2020	FERC approved TOP-003-4. Docket No. RD20-4-000	
5	May 2021	Changes pursuant to Project 2019-06	Revised
5	June 11, 2021	Board approved	Project 2019-06 Cold Weather
5	August 24, 2021	FERC approved TOP –003-5 Docket No. RD21-5-000, Order 176	
6	TBD	Adopted by NERC Board of Trustees	Revisions under project 2021-06
6.1	Errata	Approved by the Standards Committee	August 23, 2023
6.1	November 2, 2023	FERC Approved TOP-003-6.1 Docket No.RD23-6-000	
6.1	November 3, 2023	Effective Date	July 1, 2025
7	December 10, 2024	Board Adopted	Revisions under Project 2022-03
7	February 26, 2025	FERC approved TOP-003-7 Docket No.RD25-5-000	
8	TBD	Adopted by the NERC Board of Trustees	Revisions to address FERC Order No. 901 directives

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard for a formal 30-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	November 13, 2024
SAR posted for comment	May 17 – June 24, 2024

Anticipated Actions	Date
30-day formal comment period with initial ballot	April 17 – May 16, 2025
20-day formal comment period with additional ballot	July – August 2025
10-day final ballot	September 2025
Board adoption	October 2025

A. Introduction

1. **Title:** Transmission Operator and Balancing Authority Data and Information Specification and Collection

2. **Number:** TOP-003-~~7~~8

3. **Purpose:** To ensure that each Transmission Operator and Balancing Authority has the data and information it needs to plan, monitor, and assess the operation of its Transmission Operator Area or Balancing Authority Area.

4. **Applicability:**

   4.1 Functional Entities:

   4.1.1 Transmission Operator

   4.1.2 Balancing Authority

   4.1.3 Generator Owner

   4.1.4 Generator Operator

   4.1.5 Transmission Owner

   4.1.6 Distribution Provider

5. **Effective Date:** See Implementation Plan for Project 2022-~~03~~02.

B. Requirements and Measures

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

1.1. A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and information, external network data and information, Inverter-based Resource (IBR)-specific data and parameters, and identification of the entities responsible for responding to the specification as deemed necessary by the Transmission Operator.

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

1.3. Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:

1.3.1. Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

1.3.2.3. current cold weather performance temperature determined by an engineering analysis.

1.4. Identification of a mutually agreeable process for resolving conflicts.

1.5. Method(s) for the entity identified in Part 1.1 to provide the data and information that includes, at a minimum, the following:~~:~~

1.5.1. Specified deadlines or periodicity in which data and information is to be provided;

1.5.2. Performance criteria for the availability and accuracy of data and information as applicable;

1.5.3. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization;

~~**1.5.3.**~~**1.5.4.** Provisions to update or correct data and information, as applicable or necessary;

~~1.5.4.~~1.5.5. A mutually agreeable format;

~~1.5.5.~~1.5.6. Mutually agreeable method(s) for securely transferring data and information.

M1. Each Transmission Operator shall make available its dated, current, in force documented specification(s) for data and information.

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

2.1. A list of data and information needed by the Balancing Authority to support its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments, including non-Bulk Electric System data and information, IBR-specific data and parameters, and external network data and information, as deemed necessary by the Balancing Authority, and identification of the entity responsible for responding to the specification.

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

2.3. Provisions for notification of BES generating unit(s) status during local forecasted cold weather to include:

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s) minimum:

2.3.2.1. design temperature; or

2.3.2.2. historical operating temperature; or

2.3.2.3. current cold weather performance temperature determined by an engineering analysis.

2.4. Identification of a mutually agreeable process in resolving conflicts;

2.5. Methods for the entity identified in Part 2.1 to provide data and information that includes at a minimum the following~~.~~:

2.5.1. Specific deadlines or periodicity in which data and information is to be provided;

2.5.2. Performance criteria for the availability and accuracy of data and

information, as applicable;

2.5.3. Requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the ERO;

~~2.5.3.~~2.5.4. Provisions to update or correct data and information, as applicable or necessary.

~~2.5.4.~~2.5.5. A mutually agreeable format.

~~2.5.5.~~2.5.6. A mutually agreeable method(s) for securely transferring data and information.

M2. Each Balancing Authority shall make available its dated, current, in force documented specification(s) for data and information.

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

M3. Each Transmission Operator shall make available evidence that it has distributed its data specification(s) to entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.

Such evidence could include, but is not limited to, web postings with an electronic notice of the posting, dated operator logs, voice recordings, postal receipts showing the recipient, date and contents, or ~~e-mail~~email records.

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

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

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

M5. Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall make available evidence that it has satisfied the obligations

of the documented specification. Such evidence could include, but is not limited to, electronic or hard copies of data transmittals or attestations of receiving entities.

C. Compliance

1. Compliance Monitoring Process

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

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

- Each Transmission Operator shall retain its dated, current, in force, documented specification for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.
- Each Balancing Authority shall retain its dated, current, in force, documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R2 and Measurement M2, as well as any documents in force since the last compliance audit.
- Each Transmission Operator shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.
- Each Balancing Authority shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Balancing Authority's analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R4 and Measurement M4.
- Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall retain evidence

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

1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R#	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Transmission Operator did not include one or two of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include three of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include four of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.	The Transmission Operator did not include any of the parts (Part 1.1 through Part 1.5) of the documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. OR, The Transmission Operator did not have a documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.
R2	The Balancing Authority did not include two or fewer of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include three of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include four of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments.	The Balancing Authority did not include any of the parts (Part 2.1 through Part 2.5) of the documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments. OR, The Balancing Authority did not have a documented specification(s) for the data and information necessary for it to perform its analysis functions,

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

R#	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Energy Reliability Assessments.	monitoring, and Near-Term Energy Reliability Assessments.	Assessments.	
R5	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet one of the parts in Requirement R1 Part1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet two of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 satisfied the obligations in the specification, but failed to meet three or more of the parts in Requirement R1 Part 1.5 or Requirement R2 Part 2.5.	The responsible entity receiving a specification(s) in Requirement R3 or R4 did not satisfy the obligations of the documented specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- 2022-02 Implementation Plan
- 2022-02 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1		Modified R1.2 Modified M1 Replaced Levels of Non-compliance with the Feb 28, BOT approved Violation Severity Levels (VSLs)	Revised
1	October 17, 2008	Adopted by NERC Board of Trustees	
1	March 17, 2011	Order issued by FERC approving TOP- 003-1 (approval effective 5/23/11)	
2	May 6, 2012	Revised under Project 2007-03	Revised
2	May 9, 2012	Adopted by Board of Trustees	Revised
3	April 2014	Changes pursuant to Project 2014-03	Revised
3	November 13, 2014	Adopted by Board of Trustees	Revisions under Project 2014-03
3	November 19, 2015	FERC approved TOP-003-3. Docket No. RM15-16-000, Order No. 817	
4	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
4	October 30, 2020	FERC approved TOP-003-4. Docket No. RD20-4-000	
5	May 2021	Changes pursuant to Project 2019-06	Revised
5	June 11, 2021	Board approved	Project 2019-06 Cold Weather
5	August 24, 2021	FERC approved TOP –003-5 Docket No. RD21-5-000, Order 176	
6	TBD	Adopted by NERC Board of Trustees	Revisions under project 2021-06
6.1	Errata	Approved by the Standards Committee	August 23, 2023
6.1	November 2, 2023	FERC Approved TOP-003-6.1 Docket No. RD23-6-000	
6.1	November 3, 2023	Effective Date	July 1, 2025
7	December 10, 2024~~TBD~~	Board Adopted~~Energy Assurance Modifications – Addition of Near-Term ERA.~~	Revisions under Project 2022-03~~ed~~
7	February 26, 2025	FERC approved TOP-003-7 Docket No.RD25-5-000	
8	TBD	Adopted by the NERC Board of Trustees	Revisions to address FERC Order No. 901 directives

Implementation Plan

Project 2022-02 Uniform Modeling Framework for IBR

Applicable Standard(s)

- Reliability Standard MOD-032-2 Data for Power System Modeling and Analysis
- Reliability Standard IRO-010-6 Reliability Coordinator Data and information Specification and Collection
- Reliability Standard TOP-003-8 Transmission Operator and Balancing Authority Data and Information Specification and Collection

Requested Retirement(s)

- Reliability Standard MOD-032-1 Data for Power System Modeling and Analysis
- Reliability Standard IRO-010-5 Reliability Coordinator Data and information Specification and Collection
- Reliability Standard TOP-003-7 Transmission Operator and Balancing Authority Data and Information Specification and Collection

Prerequisite Standard(s)

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

- None

Applicable Entities

- Reliability Coordinator
- Balancing Authority
- Distribution Provider
- Generator Owner
- Generator Operator
- Planning Coordinator
- Resource Planner
- Transmission Owner
- Transmission Operator
- Transmission Planner
- Transmission Service Provider

NERC Glossary of Terms

This section includes a newly defined term used in the NERC Reliability Standards. The new definition listed below becomes approved when the proposed standard is approved. When the standard becomes effective, the defined term will be removed from the individual standard and added to the NERC Glossary of Terms.

Proposed New Definition:
Distributed Energy Resource (DER):
Generators and energy storage technologies connected to a distribution system that are capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including those connected behind the meter of an end-use customer that is supplied from a distribution system.

Background

As the penetration of DERs continues to increase across the many distribution systems connected both directly and indirectly to the North American Bulk-Power System (BPS), it is necessary to account for the potential impacts of DERs on reliability in the planning, operation, and design of the Bulk Electric System. The NERC System Planning Impacts of Distributed Energy Resources Working Group (SPIDERWG) has identified the need for improved modeling of aggregate DER for planning studies (including both utility-scale and retail-scale DER) conducted by Transmission Planners (TPs) and Planning Coordinators (PCs), including updated modeling data requirements specific to DER.

Further, in Order No. 901,[1] the U.S. Federal Energy Regulatory Commission ("FERC") found that it is imperative for NERC to develop new or modified Reliability Standards MOD-032, IRO-010, and TOP-003 to address reliability concerns "related to IBRs at all stages of interconnection, planning, and operations."[2]. Among other things, FERC directed NERC to develop requirements addressing the provision of IBR and DER data to the entities responsible for the planning and operation of the BPS. Detailed information on the specific FERC Order No. 901 directives addressed through this project is available in Project 2022-02 Consideration of Order No. 901 Directives.

Proposed Reliability Standard MOD-032-2 replaces the Load-Serving Entity as an applicable entity with the Distribution Provider and updates Attachment 1: Data Reporting Requirements with data specific to DERs and IBRs, consistent with addressing the FERC Order No. 901 directives. Proposed Reliability Standard MOD-032-2 also adds a new Part 1.2 in Requirement R1, which would require the Planning Coordinator and Transmission Planner to include in their data requirements and procedures requirements for model submissions in accordance with the Criteria for Acceptable Models maintained by the Electric Reliability Organization (ERO). New Requirement R2 Part 2.1 addresses estimation of unregistered IBR or DER data where actual data is not available, consistent with the directives in Order No. 901.
Revisions in the Reliability Standards TOP-003-8 and IRO-010-6 data specification standards specify that entities responsible for developing and distributing data specifications shall include requirements

[1] Reliability Standards to Address Inverter-Based Resources, Order No. 901, 185 FERC ¶ 61,042 (2023).
[2] Id. at P 25

for model submissions in accordance with the Criteria for Acceptable Models List maintained by the ERO.

General Considerations

In developing this implementation plan, the drafting team (DT) considered the time in MOD-032-2 that would be necessary to develop data requirements and reporting procedures, including identifying the proper reporting entity, for data related to IBRs, including unregistered IBRs and DERs. The DT also considered that the standard would become applicable to the Distribution Provider (DP) for the first time. Transmission Owners (TOs) and DPs would be expected to participate in PC/TP processes to change data reporting requirements related to DER and IBR developed during the 24 months prior to the effective date of Requirement R1 and should be able to start working on data collection processes and methods prior to the compliance dates of Requirements R2, R3, and R4. This timeline also allows for the development of new data estimation processes developed under MOD-032-2 Requirement R2 Part 2.1. Requirements adjusted in Reliability Standards IRO-010-5 and TOP-003-8 may not be practical to implement prior to full implementation of MOD-032-2, and therefore was set to the same timeline. One additional limitation the DT noted is the requirement for all FERC Order No. 901 directives to be fully implemented by January 1, 2030, including those covered by these standard revisions.

In summary, this implementation plan would provide a full 36 months for MOD-032 Requirements R2, R3, R4, IRO-010, and TOP-003 from FERC approval until data is required to be reported.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard and NERC Glossary term Distributed Energy Resource is provided below. Where the DT identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for those particular sections represents the date that entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Initial Performance Dates

Entities shall not be required to comply with Reliability Standard MOD-032-2 Requirements R2, R3, and R4 relating to revised Planning Coordinator/Transmission Planner data requirements and reporting procedures as developed under Requirement R1 and Attachment 1, until 12 months after the effective date of Reliability Standard MOD-032-2.

Entities shall continue to comply with Requirements R2, R3, and R4 related to Planning Coordinator/Transmission Planner data requirements and reporting procedures developed under MOD-032-1 Requirement R1 and Attachment 1 during the phased-in compliance period for MOD-032-2 unless they are compliant with revised Planning Coordinator/Transmission Planner data requirements and reporting procedures under Reliability Standard MOD-032-2 Requirement R1.

Reliability Standard MOD-032-2

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 twenty-four (24) 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 twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for Reliability Standard MOD-032-2 Requirements R2, R3, and R4

Entities shall not be required to comply with Requirements R2, R3, and R4 relating to revised Planning Coordinator and Transmission Planner data requirements and reporting procedures developed under MOD-032-2 Requirement R1 and Attachment 1 until 12 months after the effective date of Reliability Standard MOD-032-2.

Definition – Distributed Energy Resource (DER)

Where approval by an applicable governmental authority is required, the definition of DER shall become effective on the first day of the first calendar quarter that is after the effective date of the applicable governmental authority's order approving Reliability Standard MOD-032-2, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter that is after the date that Reliability Standard MOD-032-2 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Reliability Standard IRO-010-5

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 thirty-six (36) 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 thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Reliability Standard TOP-003-8

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 thirty-six (36) 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 thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

Reliability Standard MOD-032-1

Reliability Standard MOD-032-1 shall be retired immediately prior to the effective date of Reliability Standard MOD-032-2 in the particular jurisdiction in which the revised standard is becoming effective.

Reliability Standard IRO-010-4

Reliability Standard IRO-010-4 shall be retired immediately prior to the effective date of Reliability Standard IRO-010-5 in the particular jurisdiction in which the revised standard is becoming effective.

Reliability Standard TOP-003-7

Reliability Standard TOP-003-7 shall be retired immediately prior to the effective date of Reliability Standard TOP-003-8 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Approved Criteria for Acceptable Models

Project 2022-02 Uniform Modeling Framework for IBR

April 2025

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

Executive Summary

The Criteria for Acceptable Models defines criteria for model submissions under the MOD-032, TOP-003, and IRO-010 Reliability Standards. Models that are submitted for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system shall meet requirements in this document.

Disclaimers

Interconnection-wide modeling requirements may differ from the requirements of specialized studies dedicated to a particular technical objective. NERC's Criteria for Acceptable Models applies to the models where NERC Reliability Standards require its use (generally for planning and operation models where multiple entities share information beyond their portion of the electric System, which includes interconnection-wide models).

Operations models shall meet the requirements in this document, provided that models for operations shall not reduce the ability of a Registered Entity to perform their Operational Planning Analyses and Real-Time Assessments (RTAs) in a timely manner. Thus, models deemed acceptable for planning purposes may be deemed unacceptable by a receiving entity for certain operations applications.

Chapter 1: Process

Updates to the Criteria for Acceptable Models

This section describes the process by which changes may be made to the Criteria for Acceptable Models or the revision processes in this document, excluding changes to the Unacceptable Models List which will be addressed in the following section.

1. Any person or entity may submit a request to the ERO to revise the Criteria for Acceptable Models. This request shall include, at a minimum:
    a. Description of the suggested revision;
    b. Technical justification for the suggested revision;
    c. Supporting documentation; and
    d. Identification of any Confidential Information as defined in Section 1500 of the NERC Rules of Procedure.
2. ERO staff shall review and evaluate the Criteria for Acceptable Models revision request, along with any group or subcommittee of the NERC Reliability and Security Technical Committee (RSTC) or its successor charged with assisting in such reviews. If no such group or subcommittee has been identified, ERO staff may work with other industry subject matter experts as needed to review and evaluate the request.
3. As part of the review process, ERO staff shall conduct a 45-day public comment period on the proposed revision request.
4. The proposed revision request, along with the results of the review, the comments received, a summary consideration of comments, and the recommended action, shall be presented to the NERC RSTC or its successor in a duly noticed public meeting.
5. The NERC RSTC may recommend the NERC Board of Trustees approve the revision request, reject the revision request, or remand the revision request for further work. If the NERC RSTC recommends approving the revision request, the NERC RSTC shall also recommend an effective date for the revision.
6. The NERC Board of Trustees, considering the recommendation of the NERC RSTC, shall approve the revision request, reject the revision request, or approve the revision request with modifications. If approved, the NERC Board of Trustees shall also approve an effective date for the revision.
7. The ERO shall provide public notice of a revision to the Criteria for Acceptable Models along with the effective date of the revision. The revised Criteria for Acceptable Models shall be posted to the NERC website and filed with FERC for informational purposes.

Updates to the Unacceptable Models List

This section describes the process by which changes may be made to the Unacceptable Models List. The following steps shall be taken to add, remove, or modify a model to the Unacceptable Models List:

1. Any person or entity may submit a request to the ERO to add or remove a model from the Unacceptable Models List. This request shall include, at a minimum:
    a. The model name;

b. Alternative model name(s), if any;

c. Organization(s) the submitting entity represents;

d. Description of the model's stated intent;

e. Request to add model as an "unacceptable" model or remove model as an "unacceptable" model;

f. Technical supporting documentation that includes the ability of the model to meet or not meet small and large disturbance behavior;

g. Identification of any Confidential Information as defined in Section 1500 of the NERC Rules of Procedure; and

h. An explanation, if any of the above technical support items are unavailable to the supporting entity.

2. ERO staff shall review and evaluate the information in the Unacceptable Models List change request, along with any group or subcommittee of the NERC RSTC or its successor charged with assisting in such reviews. If no such group or subcommittee has been identified, ERO staff may work with other industry subject matter experts as needed to review and evaluate the request.

3. If the request is seeking to add a model to the Unacceptable Models List, ERO staff shall provide public notice that identifies the model being considered for addition to the list, includes a non-confidential summary of the rationale offered for its inclusion, and provides at least 30 days to submit comments.

4. The results of this review and the recommended action shall be presented to the NERC RSTC or its successor in a duly noticed public meeting.

5. The NERC RSTC may recommend the NERC Vice President of Engineering and Standards[1] approve the change request, reject the change request, or remand the application back to the ERO to work with the submitting entity. If the NERC RSTC recommends approving the change request, the NERC RSTC shall also recommend an effective date for the change.

6. The NERC Vice President of Engineering and Standards, considering the recommendation of the NERC RSTC, shall approve the change request, reject the change request, or remand the application back to ERO staff to work with the submitting entity. If approved, the NERC Vice President of Engineering and Standards shall also determine the effective date for the change.

7. The ERO shall provide public notice of a change to the Unacceptable Models List included in this Approved Criteria for Acceptable Models along with the effective date of the change. The revised document shall be posted to the NERC website and filed with FERC for informational purposes.

8. Technical Rationale for each model added to the Unacceptable Models List shall be retained by the ERO for as long as practicable, but no fewer than five (5) years from the date a model is added to the list.

[1] This may include an equivalent NERC officer if by a different title, or their designee.

Chapter 2: ERO Approved Criteria

Planning Models

Models that are submitted for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system shall qualify with the following:

1. All models shall be representative of expected or as-built facilities.
2. All models shall be usable (see usability requirements below).
3. All standard library models are deemed acceptable until demonstrated to not meet usability requirements and/or demonstrated to be unable to represent the expected or as-built facilities.[2]
4. Models listed on the Unacceptable Model List shall not be used unless it is demonstrated that such a model represents the expected or as-built facilities with negligible error(s) in both small signal and large disturbance behavior and does not introduce numerical instability in the software used by TPs or PCs. In these cases, the model submitting entity may submit a request to update the Unacceptable Model List. A model may be used pending the disposition of the request.

Operational Models

Models that are submitted for development of operation cases necessary to support analysis of the reliability of the interconnected transmission system shall qualify with the following:

1. All models shall be representative of expected or as-built facilities.
2. All models shall be usable (see usability requirements below).
3. All standard library models are deemed acceptable until demonstrated to not meet usability requirements and/or demonstrated to be unable to represent the expected or as-built facilities.[3]
4. Models listed on the Unacceptable Model List shall not be used unless it is demonstrated that such a model represents the expected or as-built facilities with negligible error(s) in both small signal and large disturbance behavior and does not introduce numerical instability in the software used by TPs or PCs. In these cases, the model submitting entity may submit a request to update the Unacceptable Model List. A model may be used pending the disposition of the request.
5. Models shall not reduce the viability of a Registered Entity's ability to perform their OPAs and RTAs in a timely manner.

Usability Requirements

Models that are used for representation of generation and system components shall have sufficient documentation for the user of the model to understand its parameters, states, and outputs into the simulation software. Usable models are those models that include, at a minimum, the following:

1. A model manual, or other documentation, with a description of all model parameters, variables, and states. The manual or other documentation shall also describe the range of validity of the model and valid use cases or studies for which the model has sufficient fidelity.
2. A procedure to use and initialize the model in dynamic simulations, including alterations to the steady-state representation.

[2] Poor model quality may stem from poor parameterization and/or poor implementation of a model from code. Poor parameterization or poor implementation of a particular model shall not be used to generalize a model's designation in the Unacceptable Model List.

[3] Poor model quality may stem from poor parameterization and/or poor implementation of a model from code. Poor parameterization or poor implementation of a particular model shall not be used to generalize a model's designation in the Unacceptable Model List.

3. Disclaimer(s) on the usability of the model for known model software or simulation domains.
4. An explanation of the model's adequacy to represent small and large disturbance behavior.
5. A list of commonly tuned parameters to align the model to site-specific settings as well as allowable tuning ranges for these parameters.

Chapter 3: Unacceptable Models List

Models that have been identified as unacceptable as list in Table 1 below. Revisions to this list may be made in accordance with the process described in "Updates to the Unacceptable Models List" above.

Table 1: Unacceptable Model List	
Known Unacceptable Model Name	**Model Description**
Renewable Energy Models	
WT3G1, WT3G2, wt3g	Generic Type 3 WTG Generator/Converter Model - Doubly-fed induction generator
WT4G1, WT4G2, wt4g	Generic Type 4 WTG Generator/Converter Model - Variable speed generator with full converter
WT3E1, wt3e	Generic Type 3 WTG Electrical Control Model
WT4E1, WT4E2, wt4e	Generic Type 4 WTG Electrical Control Model
WT3T1, wt3t	Generic Type 3 WTG Turbine Model
WT3P1, wt3p	Generic Type 3 WTG Pitch Control Model
WT12A1, wt1p, wt2p	Generic Type 1 and 2 WTG Pitch Control Model
WT4E1, wt4t	Generic Type 4 WTG Power Converter Model
wt4p	Generic Type 4 Pitch Control Model
REECB1, REECBU1, reec_b	Generic Phase 2 PV Electrical Controls Model
Machine Models	
GENSAL, gensal	Salient Pole Generator Model (IEEE Std 1110 §5.3.1 Model 2.1)
GENCLS, gencls	Classical Generator Model (IEEE Std 1110 §5.4.2)
GENTRA	Transient Level Generator Model
Excitation System Models	
texs	General Purpose Transformer Fed Excitation System
SEXS, sexs	Simplified Excitation System
EX2000	GE EX2000 Excitation System
Turbine-Governor Models	
lm2500	LM 2500 Aero-Derivative Gas Turbine Governor Model
lm6000	LM 6000 Aero-Derivative Gas Turbine Governor Model
URGS3T, gast	WECC Gas Turbine Governor Model
GAST	Gas Turbine-Governor Model
GAST2A	Gas Turbine-Governor Model
GASTWD	Gas turbine-governor
IEEEG2	1981 IEEE Type 2 General Approx. Linear Ideal Hydro Model
WESGOV	Westinghouse Digital Governor Model for Gas Turbines
Load Models	
motorc	Phasor Model of Single-Phase Air-Conditioner Compressor Motor

Chapter 4: Form Revisions

This form is a sample to explain what is deemed a full application to change a model designation in the NERC Approved Model Criteria for Acceptable Models List.

Name of Person submitting			
Organization(s):			
Sector (if known)			
Telephone		Email	

Model Name	
Alternative Model Name(s) as implemented in software	
Equipment Model is stated to represent	
Indicate desired Action	☐ Add "model to the Unacceptable Models List, Section X of the Approved Model Criteria for Acceptable Models ☐ Remove model from the Unacceptable Models List, Section X of the Approved Model Criteria for Acceptable Models

Description of model ability to meet small signal Disturbances	
Description of model ability to meet large signal Disturbances	
Please cite and link any industry approved documentation regarding this model's small and large signal disturbances	
Describe the technical document attachments that support the above questions	
Please identify any information in this application that may meet the criteria for Confidential Information, as defined in Section 1500 of the NERC Rules of Procedure.	

Section 4: Process Tracking	
Date Submitted to ERO	
Model Status	☐ Submitted to the ERO ☐ Assigned ERO Review team ☐ Investigation and review by ERO and submitting entity ☐ Remanded by NERC RSTC (or its successor) ☐ Approved by the NERC RSTC (or its successor)
Date of Approval	
Date of Model Notice to Industry	

Attachments:

If available, please include at least one report that demonstrates the ability or inability of the model to meet its stated purpose using Hardware-in-the-Loop, Software-in-the-Loop, or actual System response (e.g., in a commissioning test) that demonstrates the ability or inability to meet the model's stated purpose. At least one attachment should detail the model's error boundaries to represent its stated equipment with the test description and procedure outlined in that report. Entities shall label any attachment that may meet the criteria for Confidential Information under NERC Rules of Procedure Section 1500, along with the basis for the designation (e.g., Confidential Business and Market Information, Critical Electric Infrastructure Information, etc.). If any of this information is not available to the supporting entity, please provide an explanation.

Chapter 5: Technical Rationale

FERC Order No. 901

This document addresses directives within Federal Energy Regulatory Commission (FERC) Order No. 901 outlining the need to use industry approved models. Pre-defining a limited set of models (i.e., a library of models) that could be used to represent generation and system components is potentially at odds with objectives to also have accurate models, especially as technology rapidly progresses. Thus, instead of specifying a limited model library, this document provides acceptability criteria for models representing generation and system components. This document is based on the *NERC Dynamic Modeling Recommendations*[4] but is standalone. Entities are encouraged to review the *NERC Dynamic Modeling Recommendations* for further consideration and technical background for this Criteria for Acceptable Models.

Operational Models

Transmission Operators (TOPs), Reliability Coordinators (RCs), and Balancing Authorities (BAs) are required to have a "documented specification for the data necessary" to perform Operational Planning Analysis (OPA), Real-Time Assessment (RTA), and Real-time Monitoring. This data specification is then distributed by the TOP, RC, and BA to entities to fulfil the data requirements and such entities provide the data in mutually agreeable format, security protocol, and process for resolving data conflicts. FERC Order No. 901 has identified that the transient dynamic performance of Inverter-based Resources (IBRs) is underrepresented in these models. However, many OPAs and RTAs do not perform a transient dynamic simulation for all credible Contingencies due to computational time constraints. As such, models for operations shall meet the same criteria for models for planning. Thus, models deemed acceptable for planning purposes may be deemed unacceptable by a receiving entity for certain operations applications.

Unacceptable Model List

As models have evolved and been implemented in software, some models have been proven to contain modeling errors, numerical issues, insufficient technical documentation, or have been phased out of use by the owners of the equipment due to the availability of better models. The unacceptable list of models shown in Table 1 below is categorized by the type of model, and as of publication, includes only PSPD models. Revisions to this list may be made in accordance with the process described in the "Updates to the Unacceptable Models List" above.

Usability Requirements

In current planning model software, most standard library models come with a list of parameters, their description, initial values, and the appropriate disclaimers. In these cases, references to the program's application manual suffices for usability requirements 1 through 3.

In addition to the content usability requirements above, any identified inability of a model to function properly within a System Model may cause a model to be deemed unacceptable until the issue is addressed and eliminated. Such software usability issues include, but are not limited to:

1. Models that restrict user selection of the machine unique identifiers (e.g., number, name, ID) beyond the inherent software limitations.
2. Models that fail to robustly initialize under reasonable initial conditions.
3. Models that cause simulation crashes or conflict with other models in a system simulation, including other instances of the same model.
4. Models that require unique folder structures that are incompatible with System Model development.
5. Models that cause numerical instability or simulation solution challenges.

[4] Available here: https://www.nerc.com/pa/RAPA/ModelAssessment/Documents/Dynamic%20Modeling%20Recommendations.pdf

Criteria Checklist Guideline

If all the checkboxes below can be attested to with evidence that the model meets these criteria, then the model at the date of delivery is deemed acceptable in accordance with this ERO Approved Criteria for Acceptable Models.

- ☐ The model name and description is not listed in the Unacceptable Model portion of the ERO Approved Criteria for Acceptable Models.
- ☐ The model is accompanied by a manual with descriptions of all model parameters, variables, and states.
- ☐ The model manual describes the range of validity of the model and valid use cases or studies for which the model has sufficient fidelity.
- ☐ The model is accompanied by a list of commonly tuned parameters for site-specific settings.
- ☐ The model is accompanied by a procedure to use and initialize the model in dynamic simulation.
- ☐ The model accompanied by an explanation of the model's adequacy to meet small and large disturbance behavior.
- ☐ The model does not place restrictions on unique identifiers (e.g., number, name, ID) used in simulation software.
- ☐ The model initializes robustly for all reasonable initial conditions and does not cause simulation crashes.
- ☐ The model does not require unique and burdensome folder structures that are incompatible with System Model development.
- ☐ The model does not cause numerical instability or simulation solution challenges.

Chapter 6: Version History

Version	Date	Action	Change Tracking
1	April 2025	Draft 1 Posting for Project 2022-02	Initial Draft

Errata to Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7 and CIP-011-4

Action

Approve the errata changes to Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7 and CIP-011-4 to correct the spelled-out term "Electronic Access Control or Monitoring System."

Background

Section 12.0 of the Standard Processes Manual 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."*

Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7 and CIP-011-4 passed the final ballot on April 12, 2024, and were presented to the Board of Trustees for adoption on May 9, 2024. These Reliability Standards are currently pending FERC approval in a petition filed on July 10, 2024.

When Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7 and CIP-011-4 were revised under Project 2016-02 Modifications to CIP Standards, the drafting team (DT) spelled out the term "Electronic Access Control or Monitoring System" in addition to the acronym EACMS in the applicability table of Requirement R1 as that was the first use of the term in each of the standards where the term appears. However, when making this revision, the DT inadvertently included "and" instead of "or" in the language. Correction of this error is necessary to align with the defined term.

Correction of this error would not change the scope or intent of the associated Reliability Standards and would have no material impact on the end users of the Reliability Standards.

Summary

NERC staff recommends the Standards Committee approve the errata changes to Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7 and CIP-011-4. Under NERC's naming convention, the errata standards will be numbered with a ".1" following each version number as follows: CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1 and CIP-011-4.1.

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

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

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

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

   4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				for unauthorized access through a physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	TBD	Approved by the Standards Committee	Errata

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

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

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

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

CIP-006-7.1 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

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

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

CIP-006-7.1 Table R2 – Visitor Control Program

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				for unauthorized access through a physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				authorized physical entry into each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	~~TBD~~5/9/24	~~Virtualization Modifications~~ Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	TBD	Approved by the Standards Committee	Errata

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions."

A. Introduction

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

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

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

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

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

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process:

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

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

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

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

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

1.4. Additional Compliance Information:
None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7.1 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions."

A. Introduction

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

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

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

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

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

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7.1 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7.1 Table R2 – Cyber Security Patch Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

   1.4. Additional Compliance Information:
   None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7.1 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7.1 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

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

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

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

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

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

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

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

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

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

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

Violation Severity Levels

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

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control ~~and~~ or Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

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

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

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

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

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

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

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

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

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

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

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

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

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7.1:

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

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process:

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

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information: None

Violation Severity Levels

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

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	defined role in the recovery plan of the updates.	including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information: None

Violation Severity Levels

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

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

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	~~TBD~~5/9/24	Adopted by the NERC Board of Trustees.~~Virtualization Modifications~~	Virtualization Modifications

Version	Date	Action	Change Tracking
7.1	~~5/9/2024~~TBD	Adopted by the NERC ~~Board of Trustees~~Standards Committee.	Errata

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

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

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

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

   4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011.1-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4.1 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

B. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

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

Standard Development Timeline

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

Description of Current Draft

This is the final draft of the proposed standard with errata.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

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): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

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

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

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

   4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011.1-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4.1 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

B. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

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

Project 2024-01 Rules of Procedure Definitions Alignment (Generator Owner and Generator Operator)

Action

Reject the IBR Registration and Standards Applicability Glossary Update Standard Authorization Request (SAR), with a written response to the submitter, given the duplicity of work already completed by this drafting team (DT), Project 2020-06 Verifications of Models and Data for Generators, Project 2022-02 Uniform Modeling Framework for IBR, and Project 2021-01 System Model Validation with IBRs.

Background

This project addresses the definitions for Generator Owner (GO) and Generator Operator (GOP) within the NERC Glossary of Terms to ensure the inclusion of inverter-based resources (IBRs) on the Bulk-Power System (BPS) that do not meet the current definition of Bulk Electric System (BES), but do meet registration criteria updated with the June 27, 2024 approved changes to the NERC Rules of Procedure. *See Order Approving Revisions to the Rules of Procedure to Register Inverter Based Resources,* 187 FERC ¶ 61,196 (2024), Docket No. RR24-2-000.

On May 15, 2024, the Standards Committee (SC) accepted the Generator Owner and Generator Operator Definition Alignment SAR that was submitted by NERC staff to align the NERC Glossary of Terms definitions of GO and GOP with the revised definitions contained in the Rules of Procedure registry criteria for GO and GOP to align with registry criteria changes. On January 22, 2025, the SC authorized drafting new or modified definitions as identified in the Generator Owner and Generator Operator Definition Alignment SAR. On March 19, 2025, the SC authorized the initial posting of modified definitions for GO and GOP and the associated Implementation Plan for a 45-day formal comment period from March 24, 2025, through May 7, 2025.

On July 17, 2024, the SC accepted an additional SAR submitted by industry stakeholders. The IBR Registration and Standards Applicability Glossary Update SAR was posted for a 35-day formal comment period, from August 13, 2024, through September 16, 2024. This SAR proposes that the Glossary definitions of Generator Owner and Generator Operator be revised to add the owners and operators of Sub-BES IBRs, consistent with the revised Registration Criteria. The SAR also proposes developing Glossary definitions for Non-Material IBRs and for IBR-Distributed Energy Resources (IBR-DERs) and should allow for ex-ante certainty regarding the compliance application of the definitions in the same way as the definition of Sub-BES IBRs.

The DT reviewed the IBR Registration and Standards Applicability Glossary Update SAR comments on March 11, 2025, and concluded that it had achieved the objective of the SAR through its proposed revisions to the GO and GOP definitions. The DT further determined that the definitions related to IBR-DER and other related non-BES IBRs are being addressed by Milestone 3 Project 2020-06 Verifications of Models and Data for Generators and Project 2022-02 Uniform Modeling Framework for IBR. The Project 2024-01 DT chairs met with the Project 2022-02 Uniform Modeling Framework for IBR DT chairs to discuss overlap with Project 2022-02 which proposes to create a DER definition that includes distribution-connected IBRs.

NERC Standard Processes Manual Section 4.2 SAR Posting provides as follows:

- The Standards Committee, once again considering the public comments received and their resolution, may then take one of the following actions:
  - Authorize drafting the proposed Reliability Standard or revisions to a Reliability Standard.
  - Reject the SAR with a written explanation to the sponsor and post that explanation.

Summary

NERC staff recommends that the SC reject the IBR Registration and Standards Applicability Glossary Update Standard Authorization Request SAR with a written response to the submitter, given the duplicity of work already completed by this drafting team (DT), Project 2020-06 Verifications of Models and Data for Generators, Project 2022-02 Uniform Modeling Framework for IBR, and Project 2021-01 System Model Validation with IBRs.

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:	IBR Registration and Standards Applicability Glossary Update		
Date Submitted:	May 17, 2024		
SAR Requester			
Name:	Brian Evans-Mongeon (TAPS), Joe McClung (LPPC), Latif Nurani (APPA), Bill Zuretti (EPSA)		
Organization:	American Public Power Association, Electric Power Supply Association, Large Public Power Council, and Transmission Access Policy Study Group		
Telephone:		Email:	lnurani@publicpower.org bzuretti@epsa.org mcclja@jea.com bevans-mongeon@tapsgroup.org

SAR Type (Check as many as apply)	
☐ New Standard ☐ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☒ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan	☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified

What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

FERC in the IBR Registration Order found that BPS-connected inverter-based resources (IBR) that do not meet the Bulk Electric System (BES) definition can have an aggregate material impact on Bulk Power System (BPS) reliability, and the owners and operators of such resources must therefore be registered and subject to NERC reliability standards. NERC has updated the Rules of Procedure (ROP) to allow for registration of the owners and operators of non-BES IBR aggregations of at least 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV ("Category 2" GOs and GOPs); these ROP changes are pending

Requested information

before FERC. FERC's Order 901 directives with respect to "registered IBRs" apply to both BES IBR facilities and those non-BES IBR facilities that meet the revised Registry Criteria thresholds. *See*, *e.g.*, Order 901 P 4 n.14. Order 901 also includes directives with respect to BPS-connected IBRs that do not meet the registration thresholds (which Order 901 refers to as "unregistered IBRs") and "IBR-DERs," i.e., distribution-connected IBRs.

To comply with Order 901's directives that both BES IBR facilities and the non-BES IBR facilities that meet the revised Registry Criteria thresholds be subject to particular standards, Standard Drafting Teams (SDTs) must be able to refer clearly to these sets of facilities in drafting standards. "BES" is already a Glossary-defined term, and a definition of "Inverter-Based Resource" is being developed, so an SDT can refer to "BES IBRs" in the facilities Applicability section of a standard and/or in particular requirements, as appropriate; no additional work is therefore needed to define BES IBRs. But there is no corresponding term for non-BES IBRs that meet the revised Registry Criteria thresholds. There is a similar need for defined terms for BPS-connected IBRs that do not meet the revised Registry Criteria thresholds and for distribution-connected IBRs.

In addition, in order to subject all "registered IBRs" to appropriate standards consistent with Order 901, the Glossary definitions of Generator Owner (GO) and Generator Operator (GOP) must be expanded to add Category 2 GOs and GOPs.[1]

Defined terms for (a) non-BES IBRs that meet the revised Registry Criteria thresholds, (b) BPS-connected IBRs that fall below the revised Registry Criteria thresholds, and (c) distribution-connected IBRs are needed to avoid confusion and delay in standards development—including Order 901 compliance—and to allow the standards to provide clarity to registered entities and enforcers regarding each standard's facilities applicability. The risk of confusion and delay is not speculative: in the absence of a defined term for non-BES IBRs that meet the revised Registry Criteria thresholds (referred to for convenience as "Sub-BES IBRs," though the SDT is free to consider an alternative term), SDTs working on Order 901 compliance projects have resorted to vague facilities applicability terms such as "BPS IBRs." Similar confusion is to be expected once work begins on the standards involving BPS-connected IBRs that fall below the revised Registry Criteria thresholds (referred to for convenience as "Non-Material IBRs," again without limiting the SDT's ability to consider an alternative term) and distribution-connected IBRs (referred to for convenience as "IBR-DERs"). There are several significant negative consequences:

1. Because ballot pool members are aware of the problems inherent in unclear standards applicability, draft standards with vague applicability terms are likely to be voted down. The Order 901 compliance deadlines and the pressing reliability need to address IBR-specific risks are such that we cannot afford to waste time on unnecessary failed ballots. SDTs and ballot pool members should be able to focus on more substantive technical issues, rather than being distracted by drafting challenges.

[1] It is, of course, also necessary to revise existing standards themselves to apply to Category 2 GO/GOPs and to those non-BES IBR facilities that meet the revised Registry Criteria thresholds, but that work is within the scope of existing Order 901 compliance standards development projects, and not proposed as part of this SAR.

Requested information

2. Absent a clear and consistent statement of applicability that is used consistently throughout a proposed standard (and across related standards), there is an increased risk that FERC would reject the standard as overly vague and noncompliant with Order 901.
3. Finally, if a standard with such vague applicability were approved by FERC and allowed to go into effect, registered entities would not know which facilities are subject to the standard, or which entities have responsibilities with respect to each facility, leading to both reliability risks and unreasonable compliance risks.
    a. An entity may be registered as a Category 2 GO/GOP based initially on one facility, but own or subsequently acquire another facility whose status vis a vis revised Registry Criteria thresholds is less clear.
    b. Pursuant to Order 901, the owners and operators of IBRs that meet the criteria for owner/operator registration must be required to "provide IBR-specific modeling data and parameters . . . that accurately represent the registered IBRs to their [PCs], [TPs], [RCs], [TOPs], and [BAs] that are responsible for planning and operating the [BPS]" (P 76). In the case of IBR facilities that do *not* meet the thresholds for owner/operator registration, however—even if the facility is owned/operated by a registered GO/GOP—the interconnecting TO or DP, not the GO/GOP, is to be the entity responsible for providing data to system planners and operators. *Id*. P 107.
        i. If an IBR facility's status is unclear, it may "fall through the cracks," with its data being reported by neither its GO/GOP owner/operator nor its interconnecting TO or DP. Alternatively, the facility could be double counted if both entities report it.
    c. This lack of clarity results in inappropriate compliance risk for GO/GOPs, and (for data and modeling standards) TOs and DPs, as these entities will not know with certainty which facilities they must be able to demonstrate compliance for.

As explained in more detail in the "Purpose or Goal" section, the risks described above would be significantly lessened by the creation of Glossary definitions for Sub-BES IBRs, Non-Material IBRs, and IBR-DERs.

Any standard or definition carries some risk of ambiguity and need for interpretation. But given the fundamental nature of the question here—whether or not a facility is subject to the suite of Order 901 "registered IBR" standards, and which registered entity is responsible for providing data and models with respect to the facility—a failure to have a consistent understanding of each facility's status would be particularly damaging, leading to reliability risk (double-counting, under-counting, etc.) and undue compliance risk. Having a clear definition as described above is vital in mitigating these risks, but to ensure a common understanding and more fully mitigate the risk, it would be worthwhile for the SDT to not only define the three sets of non-BES IBRs, but also go another step by providing *ex ante* clarity to affected registered entities and CMEP staff regarding which facilities meet each new definition.

Because the first set of standards dealing with Category 2 GO/GOPs and Sub-BES IBRs must be submitted to FERC by November 4, 2024, while standards affecting the other two sets of IBRs are due in November 2025, it is proposed that this project take place in two phases, so that revisions to the GO/GOP definitions and the new defined term for Sub-BES IBRs can be developed on an expedited

Requested information
timeline, followed by Phase 2 addressing BPS-connected IBRs that fall below the revised Registry Criteria thresholds and IBR-DERs.
Purpose or Goal (What are the reliability gap(s) or risk(s) to the Bulk Electric System being addressed, and how does this proposed project provide the reliability-related benefit described above?):
To facilitate standards drafting and clarify standards applicability, Phase 1 of the proposed project should develop a definition of Sub-BES IBRs. (As noted above, the SDT is free to consider another term instead). SDTs working on Order 901 compliance projects or other standards development projects would then be able to use the Sub-BES IBR definition in standards; for example, a Facilities Applicability section could state that the standard applies to "BES IBRs and Sub-BES IBRs"; a requirement could state that a GO should take a certain action with respect to each BES IBR and Sub-BES IBR that it owns. In developing a definition of Sub-BES IBRs, the SDT should attempt to provide affected registered entities and CMEP staff with ex ante certainty regarding which IBR facilities qualify as Sub-BES IBRs. This could be done within the Glossary definition itself or via a new or revised Reliability Standard; and/or, if necessary, via recommending changes to NERC's Rules of Procedure. 1. For example, rather than simply setting out the thresholds, the Glossary definition could be based on whether there has been a written determination by the applicable Regional Entity that a facility meets the thresholds (e.g., "As determined by the Regional Entity in written notice transmitted to the entity(ies) that own(s) the facility at the time the determination is made, non-BES inverter-based generating resources that aggregate to a total nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV.") a. Alternatively, to avoid overburdening Regional Entities, the definition could track the process set out for BES determinations, in which "in the absence of bad faith, if a registered entity applies the [BES] definition and determines that an element no longer qualifies as part of the [BES], upon notifying the appropriate Regional Entity that the element is no longer part of the [BES] the element should not be treated as part of the [BES] unless NERC makes a contrary determination in the exception process." FERC Order 773-A P 110. b. Either of these approaches would likely require changes to Appendix 5C of NERC's Rules of Procedure to make the BES Exceptions Process applicable to determinations of Sub-BES IBR status. 2. Alternatively, a Reliability Standard approach could be modeled on the CIP-002 approach to BES Cyber System categorization. Phase 1 of the proposed project should also update the Glossary definitions of Generator Owner and Generator Operator to add the owners and operators of Sub-BES IBRs, consistent with the revised Registration Criteria. The challenge, however, is that expanding the GO and GOP categories—which are already subject to existing standards—in this manner will subject newly-registered "Category 2" GOs and GOPs to the full set of GO/GOP standards (although such entities may not own/operate any

Requested information
facilities to which some GO/GOP standards apply).[2] Section 5.1 of the Standard Processes Manual requires that "If a term has already been defined, any proposal to modify or delete that term shall consider all uses of the definition in approved Reliability Standards, with a goal of determining whether the proposed modification is acceptable, and whether the proposed modification would change the scope or intent of any approved Reliability Standards." It goes on to state that "[a]ny definition that is balloted separately from a proposed new or modified Reliability Standard or from a proposal for retirement of a Reliability Standard shall be accompanied by an implementation plan." Accordingly, the SDT must consider the impact of the expansion of the GO and GOP definitions on each existing standard that applies to GO and/or GOP, and must propose an appropriate implementation plan in light of those impacts. If the SDT determines that the expansion of the definitions of GO and/or GOP would inappropriately expand the applicability of a particular standard, the SDT should propose changes to the standard(s) at issue or, if the standard at issue is being revised by another drafting team in compliance with Order 901, should publicly notify the applicable SDT of its recommendation and account in its implementation plan for the time needed for such additional standards revisions.[3] Phase 2 of the project should develop Glossary definitions for Non-Material IBRs and for IBR-DERs, and should allow for *ex ante* certainty regarding the application of the definitions in the same way as the definition of Sub-BES IBRs. In order to comply with Order 901's differing directives regarding Non-Material (BPS-connected) IBRs and IBR-DERs, the SDT will need to attempt to distinguish between "BPS-connected" and "distribution connected" IBRs. Consistent with the Category 2 GO/GOP registration thresholds, 60 kV may be a reasonable place to draw the line. But because "Bulk Power System" and "local distribution" are both statutory terms affecting FERC's jurisdiction, it will likely be necessary to account for the possibility of case-by-case jurisdictional determinations by FERC, similar to FERC "local distribution" determinations in the context of the BES definition. Neither phase of this project is intended to result in any registered entity being subject to compliance with respect to Non-Material IBRs or IBR-DERs, although other standards projects are expected to use the definitions developed by this project in developing standards to apply to data and models of such facilities.

[2] As discussed below, NERC Staff has submitted a draft SAR to revise the GO/GOP Glossary definitions ("NERC Staff SAR"), and it is requested that this SAR be assigned to the same Standard Drafting Team as the NERC Staff SAR. The NERC Staff SAR includes an initial list of standards that may become applicable to Category 2 GOs and/or GOPs and to their non-BES facilities as a result of the expansion of the GO/GOP definitions. It will of course be necessary for the SDT to perform an independent review, using the SAR list as a starting point.

[3] For example, as noted above, Order 901 directs that where "unregistered IBRs" and IBR-DERs are owned/operated by a registered GO/GOP, the interconnecting TO or DP, not the registered owner/operator, should be responsible for providing data regarding the unregistered IBRs and IBR-DERs. The SDT may determine that in the absence of additional changes to MOD-032, TOP-003, and/or IRO-010, the expansion of the GO/GOP categories would result in those standards being interpreted to require registered GO/GOPs to provide data on *all* of their non-BES generation, contrary to Order 901's directive. *See* February 2024 Board of Trustees Agenda Package, pdf p. 275, stating that expansion of the GO/GOP categories will make "IRO-010 and TOP-003 applicable with Glossary update without further revision." Because TOP-003-5 Requirements R3-R5 and IRO-010-3 do not include explicit facilities applicability, if they are interpreted to apply to *some* non-BES facilities (i.e., those IBR aggregations that meet the revised Registry Criteria thresholds), it is unclear why they would not apply to *all* non-BES generation, including IBR aggregations that do not meet the revised thresholds and non-BES synchronous generation.

Requested information
Project Scope (Define the parameters of the proposed project):

Phase 1:

1. Reduce potential for confusion regarding applicability of standards to non-BES IBRs:
    a. Develop a definition for Sub-BES IBRs, i.e., non-BES IBR aggregations meeting the Registry Criteria thresholds. If the SDT determines that another approach (a different Glossary term and/or Reliability Standards revisions) would more effectively provide clarity and transparency regarding non-BES IBR standards applicability in standards drafting and compliance, the SDT may pursue that alternative approach instead of or in addition to defining Sub-BES IBRs.
    b. If possible (either in the Glossary definition itself or via a new or revised Reliability Standard, or, if necessary, via a recommended change to NERC's Rules of Procedure), provide for ex ante certainty regarding which IBR facilities are Sub-BES IBRs.
2. Update GO/GOP definitions:
    a. Update the Glossary definitions of Generator Owner and Generator Operator to add the owners and operators of Sub-BES IBRs. (In the drafting team's discretion, in light of the time available and the team's judgment of the potential for controversy, the Glossary definitions may either (i) be made verbatim identical to the revised ROP definitions or (ii) incorporate the defined term "Sub-BES IBRs," or other equivalent term developed by the SDT to refer to the facilities that meet the revised Registry Criteria thresholds.)
    b. Propose an appropriate implementation plan for the revised GO/GOP definitions.
    c. The SDT should ensure that expansion of the GO/GOP definitions does not result in an inappropriate expansion of the facilities applicability of any existing standard. If necessary to avoid such an unintended consequence, the SDT should propose appropriate revisions to the standard(s) at issue or, if the standard is being revised by another project in compliance with Order 901, recommend such changes to the applicable SDT and account in its implementation plan for the time needed for the additional standards revisions.
    d. This project is *not* intended to determine appropriate thresholds, because proposed thresholds are pending before FERC in the form of the revised Registration Criteria. To the extent that FERC directs changes to the proposed thresholds, this drafting team should incorporate those changes into its proposal.

Phase 2:

1. Reduce potential for confusion regarding applicability of standards to non-BES IBRs
    a. Develop definitions for (i) Non-Material IBRs, i.e., BPS-connected IBRs that do not meet the revised Registry Criteria thresholds, and (ii) IBR-DERs, i.e., distribution-connected IBRs. If the SDT determines that another approach (different Glossary term(s) and/or Reliability Standards revisions) would more effectively provide clarity and transparency regarding non-BES IBR standards applicability in standards drafting and compliance, the SDT may pursue that alternative approach instead of or in addition to defining Non-Material IBRs and IBR-DERs.
    b. If possible (either in the Glossary definition itself or via a new or revised Reliability Standard, or, if necessary, via a recommended change to NERC's Rules of Procedure),

Requested information
provide for ex ante certainty regarding whether a given non-BES IBR facility is a Sub-BES IBR, Non-Material IBR, or IBR-DER.
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[4] of developing a new or revised Reliability Standard or definition, which includes a discussion of the risk and impact to reliability-of the BES, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
1. The deliverables *must* include Glossary definitions of (a) IBR facilities that meet the new registration thresholds, (b) BPS-connected IBR facilities that fall below the new registration thresholds, and (c) distribution-connected IBRs (or other approach that addresses the problem of confusion regarding standards applicability to such classes of IBR facilities). 2. The deliverables *must* also include revisions to the Glossary definitions of GO and GOP to add the owners and operators of Sub-BES IBRs, with an appropriate implementation plan. 3. If possible, the deliverables *should* also include (via text in the proposed Glossary definition or a new/revised standard) some means of providing ex ante certainty regarding which non-BES IBR facilities meet each new definition. 4. *If necessary*, the deliverables *must* include revisions to affected standards to avoid inappropriate changes to standards applicability as a result of the expansion of the GO/GOP definitions, or recommendations that another pending project make such revisions. Technical foundation documents include (or will include): 1. IBR Registration Order 2. Order 901 3. FERC order on revisions to Statement of Compliance Registry Criteria (not yet issued as of the date of submission of this draft SAR) Subject to the binding nature of FERC orders, including Order 901, it is the SDT's responsibility to exercise its independent judgment regarding (a) the impact on standards applicability of expanding the GO/GOP definitions and (b) whether, and if so, on what implementation timeframe, any impacted standards *should* apply to Category 2 GO/GOPs and Sub-BES IBRs.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Adding newly registered "Category 2" GOs and GOPs to the Glossary definitions of GO and GOP is necessary for compliance with the IBR Registration Order and Order 901, which do not include cost estimates. However, the approach proposed in this SAR would minimize the confusion associated with complying with FERC's directives and thus minimize the burden on registered entities and the ERO.

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

Requested information
Similarly, the addition of defined terms for each of Order 901's three classes of non-BES IBR facilities will simplify standards drafting (including in response to Order 901 directives) and registered entity compliance with the resulting standards, decreasing the costs and risks associated with those activities.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):

No BES facilities will be impacted by the proposed project; by design, the proposed project will address only *non*-BES IBR facilities.
Unique characteristics of impacted facilities:
• Many Sub-BES IBRs, Non-Material IBRs, and IBR-DERs are dispersed and/or variable.
• Affected resources may include hybrid aggregations, including:
  ○ IBR/IBR (e.g., solar/battery storage) hybrids; and
  ○ the IBR portion of IBR/non-IBR (e.g., gas/battery storage) hybrids.

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 NERC Rules of Procedure Appendix 5A:
Glossary terms will directly affect GOs and GOPs and will affect the compliance responsibilities of TOs and DPs.
Do you know of any consensus building activities[5] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This proposal has been vetted by several trade associations and their members and revised and improved based on discussions with those entities. The most significant improvement resulting from those discussions is the addition of the proposal to develop definitions of Non-Material IBRs and IBR-DERs.
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)?
As noted above, NERC Staff has submitted a draft SAR to revise the GO/GOP Glossary definitions ("NERC Staff SAR"). We request that the Standards Committee assign this SAR to the same SDT as the NERC Staff SAR, and that the SDT merge the two SARs. As discussed above, development of defined terms for Sub-BES IBRs, Non-Material IBRs, and IBR-DERs is both necessary and urgent. And given the very close relationship between the proposed new IBR facilities definitions and the proposed revisions to the GO/GOP entity definitions, it would be most efficient for these efforts to be handled as a single project. Assigning the two SARs to the same SDT and merging them will eliminate the need for coordination between two separate SDTs, saving time and significantly reducing the potential for conflicting proposals.

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

Requested information
Part of the SDT's responsibilities will include reviewing all standards applicable to GOs and GOPs to determine the appropriate implementation period(s) for the expansion of the definitions of GO and GOP. Affected standards likely include, among others, IRO-010, MOD-032, and TOP-003. Affected projects may include the following Order 901 compliance projects: 2020-02 Modifications to PRC-024 (Generator Ride-through); 2020-06 Verifications of Models and Data for Generators; 2021-04 Modifications to PRC-002-2; 2023-02 Analysis and Mitigation of BES Inverter-Based Resource Performance Issues; 2021-01 Modifications to MOD-025 and PRC-019; 2023-01 EOP-004 IBR Event Reporting; 2021-02 Modifications to VAR-002-4.1; 2022-02 Modifications to TPL-001-5.1 and MOD-032-1; 2022-04 EMT Modeling; and 2023-05 Modifications to FAC-001 and FAC-002.
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 with the benefits of using them.
A somewhat lower-effort approach would be to adopt the new Rules of Procedure definitions of GO and GOP into the Glossary, *without* developing defined terms for Order 901's three classes of non-BES IBR facilities. Such an approach is incomplete, however, because (a) by omitting development of defined terms for affected IBR facilities, the alternative approach would fail to remedy the significant existing confusion in standards drafting, and significant potential confusion in standards compliance, regarding such facilities; and (b) the alternative approach would not avoid the most resource-intensive aspect of the project: the need for the SDT to review all standards affected by the expansion of the GO and GOP definitions (i.e., all standards applicable to GO and/or GOP) and develop an appropriate implementation plan.

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.

Reliability Principles	
☐	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 ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document
Risk Tracking.	
☐ Grid Transformation ☐ Resilience/Extreme Events	☐ Energy Policy ☐ Critical Infrastructure Interdependencies
☐ Security Risks	

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer
5	August 14, 2023	Standards Development Staff	Updated template as part of Standards Process Stakeholder Engagement Group

Canadian-specific Revisions to EOP-012-3 – Extreme Cold Weather Preparedness and Operations

Action

- Accept the Canadian-specific Revisions to EOP-012-3 – Extreme Cold Weather Preparedness and Operations Standard Authorization Request (SAR)
- Authorize posting of the SAR for 30-day formal comment period; and
- Authorize solicitation of drafting team (DT) members.

Background

Registered entities from across Canada have stated that the EOP-012 Reliability Standard poses compliance difficulties for Canadian entities due to the differences between Canadian and United States. regulatory environments. Canadian entities have also identified issues with how the EOP-012 standard may be applied in their consistently cold climates. This SAR seeks Canadian-specific revisions to the proposed EOP-012-3 Reliability Standard that would be designed to reflect the geographical differences that are present in Canada where peak demand typically occurs during winter months and where generating units are economically constrained to be suitable for winter operation and address differences in regulatory frameworks that make several of the FERC-directed changes in EOP-012 for the U.S. impractical to implement in the Canadian jurisdictions.

Summary

NERC staff recommends that the Standards Committee (SC) accept the Canadian-specific Revisions to EOP-012-3 – Extreme Cold Weather Preparedness and Operations SAR, authorize posting the SAR for a 30-day formal comment period, and authorize the solicitation of DT members.

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:	Canadian-specific Revision to proposed standard EOP-012-3 – Extreme Cold Weather Preparedness and Operations		
Date Submitted:	March 14, 2025		
SAR Requester			
Name:	Alexandre Bertrand, (Hydro-Québec), Constantin Chitescu (Ontario Power Generation), Jeffrey Streifling (NB Power), Kristy Lee Young (Manitoba Hydro), Abbas Munir (Bruce Power)		
Organization:	Electricity Canada Members from Québec (Hydro-Québec), Ontario (Ontario Power Generation and Bruce Power), New Brunswick (New Brunswick Power Corporation) and Manitoba (Manitoba Hydro)		
Telephone:		Email:	
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	
What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Registered entities from across Canada have indicated that given the fact that Canadian entities successfully operate in below-freezing temperatures for up to six (6) months of the year, extreme cold weather does not jeopardize the reliable operation of the power system in Canada as described by the Federal Energy Regulatory Commission (FERC), NERC, and Regional Entity Joint Staff Report (the "Report") into the February 2021 extreme cold weather event that occurred in the southwest United States. Consequently, due to current practices and mitigation efforts, extreme cold weather has not jeopardized the reliable operation to the power system in Canada.			

Requested information
Ultimately, the existing EOP-012 reliability standard's intention of addressing reliability-related findings from the Report poses difficulties for Canadian entities caused by differences between Canadian and US regulatory environments Accordingly, this Canadian-specific revision to proposed EOP-012 Reliability Standard aims to more appropriately reflect the geographical differences where Canadian peak demand typically occurs during winter months and where Canadian generating units are economically constrained to be suitable for winter operation. This Canadian-specific revision to the EOP-012 standard also aims to more appropriately reflect regulatory practices and processes in Canada.
Purpose or Goal (What are the reliability gap(s) or risk(s) to the Bulk Electric System being addressed, and how does this proposed project provide the reliability-related benefit described above?):
Registered Canadian entities from the provinces of Québec, Ontario, New Brunswick, and Manitoba have indicated support in developing an Extreme Cold Weather Preparedness and Operations Reliability Standard that aligns with provincial regulatory practices and processes and considers their unique climatic conditions. These Canadian Registered Entities have extensive experience on mitigating the reliability impact of extreme cold weather on their power systems and this approach has ensured that the Bulk Electric System (BES) remains reliable and resilient during extreme cold weather conditions, ultimately benefiting the overall reliability of the electric system in North America. The goal of this SAR is to better reflect the following Canadian specificities: 1. Canadian Registered Entities regulatory practices and processes that vary from province to province. The current EOP-012-3 Reliability Standard should be revised to allow Canadian jurisdictions to define Canadian-specific language that is needed to align with the regulatory practices and processes for each province when it comes to the development, approval, implementation and extensions requests of Corrective Action Plans (CAPs) and Generator Cold Weather Constraint declarations. 2. Geographical and winter climatic characteristics of the Canadian provinces, including operating in remote areas, require revisions to the EOP-012 Reliability Standard to allow Canadian Registered Entities to define and implement an alternative Extreme Cold Weather Temperature (ECWT) and Generator Cold Weather Reliability Event (GCWRE) on applicable units in locations where operating temperatures are well below the freezing point during the coldest time of the year. 3. The current language of apparent cause(s) due to freezing of equipment or impacts of freezing precipitation in the GCWRE definition needs to better focus investigation efforts on addressable cold-weather events that will lead to reliability improvements, efficiently excluding events that just happen to occur during cold-weather but are not cold-weather related and are therefore outside of the scope of this EOP-012-3 standard. This variance shall be applicable in those Canadian jurisdictions where the variance has been approved for use by the applicable governmental authority or has otherwise become effective in the jurisdiction.

Requested information
Project Scope (Define the parameters of the proposed project):
The EOP-012 Extreme Cold Weather Preparedness and Operations Reliability Standard should be revised to allow Canadian jurisdictions to account for the following: • The EOP-012 Reliability Standard should be updated to reflect Canadian-specific language regarding applicable governmental authorities and their applicable processes, where applicable, when it comes to development, approval, implementation and extensions requests for CAPS and Generator Cold Weather Constraint declarations. • The EOP-012 Reliability Standard document should be updated to account for the environmental geographical differences specific to non-US entities, including allowing additional flexibility in the definition of ECWT and GCWRE. • The EOP-012 Reliability Standard should be updated to address the difference between freezing risk and cold temperature operating risk where the operating temperature is far below the freezing point. • The EOP-012- Reliability Standard should ensure that all new or modified requirements do not impose retroactive compliance obligations as result of differences in the standard effective dates for non-US entities by clearly specifying an enforcement date starting with the standard effective date in Canadian specific jurisdictions. • Modify or remove language that implies modification, construction or enhancement of facilities requiring economic investment. For example, in Manitoba, the Manitoba Hydro Act, C.C.S.M. c. H190, requires that a reliability standard adopted may not: (a) have the effect of requiring the construction or enhancement of facilities in Manitoba; (b) apply to facilities in Manitoba that do not materially affect the regional electricity grid; or (c) relate to the adequacy of generation resources for Manitoba. As currently written, R6 6.3.2, 6.3.5, R7 and R8 of the EOP-012-3 draft standard fall under (a) above, which would preclude Manitoba from adopting this standard.
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] of developing a new or revised Reliability Standard or definition, which includes a discussion of the risk and impact to reliability-of the BES, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
NERC has spent a substantial amount of time and effort working with the industry to develop a FERC Order directed continent-wide extreme cold weather preparedness and operations Reliability Standard. The drafting team responsible for the development of the Canadian variance to the EOP-012 reliability standard shall address the points below: 1. Canadian entities request that Canadian-specific revisions to the EOP-012 Reliability Standard recognize that they operate at different meteorological conditions that are routinely at temperatures close to their respective ECWT for extensive durations. Consequently, we request that the EOP-012 reliability standard provide the flexibility for Canadian jurisdictions to leverage

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

Requested information

their expertise and to build on their cold weather impact assessment methodologies to define alternative Extreme Cold Weather Events targeted to their unique climatic conditions.

2. Canadian entities have a concern with Requirement R2, applicable to generating units that begin commercial operation between October 1, 2027, and March 31, 2028, for which the Generator Owner first contractually committed to design criteria relevant to the requirement before June 29, 2023.

   Footnotes 4 and 6 for EOP-012 Requirement R2.1 state, "in non-U.S. jurisdictions, use the date the applicable government authority in the relevant jurisdiction approved the first version of the EOP-012 Reliability Standard and the definition of ECWT," does not adequately reflect the differing provincial filing and enforcement processes. This SAR intends to use the effective date for the new Canadian-specific revision to the EOP-012 Reliability Standard, for non-US entities, as the applicability criteria for the Generator Owner first contractual commitment to design criteria, thus avoiding any confusion over implementation dates and retroactively imposing compliance obligations through new or revised requirements.

3. A concern with Requirement R6 is that the definition of GCWRE "apparent cause" is so broad that potentially half or more of all forced outages, derates, and startup failures may have to be investigated to rule out 'freezing of equipment' and 'impacts of freezing precipitation', since Canadian entities may operate below freezing temperatures for 6 months per year. Many outages, derates, and start-up failures would have no relationship to the fact that the weather happens to be below freezing when they occur, and an implicit requirement to investigate all outages and derates to rule out freezing equipment and freezing precipitation as causes would result in a disproportionate compliance burden on Canadian entities in regards to documenting which event is a cold weather event that would require a CAP and how to differentiate these events from other outages. A Canadian variance should allow a narrower definition of GCWRE to focus investigation efforts on events that are likely to have cold-weather related causes and thereby target investigation efforts on events that would be more likely to lead to reliability improvements.
4. The SAR should update the EOP-012 Reliability Standard to account for the environmental and geographical differences specific for Canadian entities. It shall be within the drafting team's purview to determine the best way to target cold-weather requirements to benefit BES reliability in Canada
5. The standard should be updated to differentiate between issues that occur around the freezing point (0C) and operating temperatures that are well below the freezing point. For Canadian entities, that routinely and for extensive durations are operating at temperatures close to their respective ECWT it is not possible to have freezing precipitation (e.g., snow, ice, and freezing rain), when the operating temperature is well below 0◦C that could impact equipment within the Generator Owner's control. The drafting team should reconsider the exacerbating cooling effect, involving impacts of freezing precipitation (e.g., sleet, snow, ice, and freezing rain) on equipment within the Generator Owner's control, to minimize unnecessary compliance burdens

Requested information
and exclude equipment with operational history at ECWT when the ECWT is for example, below -5◦C. The Canadian-specific revision of EOP-012 should account for the fact that the 'freezing precipitation' phenomenon (freezing rain, ice pellets, etc.) occurs near 0°C, while ECWTs and system peak loads may occur at much colder temperatures, at which the only precipitation that occurs is fluffy snow which typically has no operational impact. In addition, the term "sleet" is not a term used by Environment Canada as it is subject to conflicting definitions in Canadian English. Canadian entities may benefit from a flexible approach to manage icing issues near 0°C, since supply adequacy issues associated with system peak loads typically occur at much colder temperatures. 6. The Canadian-specific revision of EOP-012 should define an alternative process for assessing Generator Cold Weather Constraint declarations and CAP extensions that would be suitable for Canadian jurisdictions in which Compliance Enforcement Authorities are not set up to process issues associated with cold weather engineering. The drafting team should also consider entities other than the CEA for evaluating the technical merits of Cold Weather Constraint declarations and CAP extensions. 7. The drafting team should address the misalignment between the requirements and the measures in R2 and R3. Measures M2 and M3 provide as sufficient evidence of compliance the identification of generating unit minimum temperatures per Part 1.2.2 being equal to or less than the unit's ECWT; however, the language in the Requirements stipulates design requirements related to wind speed, operational dates, etc., that appears to be more stringent than the requirement implicit in the measures that the generating unit minimum temperature merely needs to be colder than the ECWT. The carveout for generating units with minimum temperatures demonstrated to be colder than the ECWT should be moved into the requirement language of R2 and/or R3.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
This SAR will better target requirements to advance BES reliability during cold conditions in Canada, as Canadian entities operate successfully within extreme cold weather almost six (6) months of the year. Implementation of CAPs as written in the current EOP-012-3 standard may not work in certain provincial regulatory frameworks by which investments are vetted and approved. The SAR will update the EOP-012 standard to appropriately reflect the regulatory frameworks that exist in affected Canadian provinces.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None identified.

Requested information
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the NERC Rules of Procedure Appendix 5A:
GO/GOP
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.
Canadian entities not subject to FERC's jurisdiction have repeatedly expressed through commenting and balloting the need for a Canadian-specific revision of the EOP-012 Reliability Standard, as well as through SDT meeting participation, and most recently during meetings between NERC, NPCC and Canadian entities. The proposed changes are well supported and reflect the unique needs and conditions of Canadian provinces.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Project 2024-03 Revisions to EOP-012-2 EOP-012-3 Extreme Cold Weather Preparedness and Operations
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 with the benefits of using them.
No alternatives have been identified.

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

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

Reliability Principles	
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

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

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

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document
Risk Tracking.	
☐ Grid Transformation ☐ Resilience/Extreme Events	☐ Energy Policy ☐ Critical Infrastructure Interdependencies
☐ Security Risks	

Version History

Version	Date	Owner	Change Tracking
1	February 12, 2025		First version

EOP-012-3 Cold Weather Update

Action
Informational.

Summary
This item is to inform the Standards Committee of the updates of EOP-012-3.

NERC Legal and Regulatory Update
March 3, 2025 – April 1, 2025

NERC FILINGS TO FERC SUBMITTED SINCE LAST SC UPDATE

FERC Docket No.	Filing Description	FERC Submittal Date
RD25-6-000	Joint Petition for Approval of Proposed Regional Reliability Standard BAL-004-WECC-4 NERC and WECC submitted a Joint Petition for Approval of Proposed Regional Reliability Standard BAL-004-WECC-4.	3/12/2025
RD24-5-000; RD24-1-000	Motion for Extension of Time NERC submitted a Motion for Extension of Time for filing the Petition for Approval of EOP-012-3 from March 27, 2025, to no later than April 14, 2025.	3/20/2025
RM18-2-000	NERC Annual Report on Cyber Security Incidents NERC submitted its Annual Report on Cyber Security Incidents.	3/21/2025
RM25-3-000	NERC Comments on PRC-029 NOPR NERC submitted Comments to FERC on the Notice of Proposed Rulemaking (NOPR) proposing to approve PRC-029-1, PRC-024-4, and the definition for “Ride-through.”	3/24/2025
RR09-6-003	2025 NERC Standards Report, Status and Timetable for Addressing Regulatory Directives NERC submitted its 2025 NERC Standards Report, Status and Timetable for Addressing Regulatory Directives. The annual report is in accordance with Section 321.6 of the NERC Rules of Procedure.	3/28/2025

FERC ISSUANCES SINCE LAST SC UPDATE

FERC Docket No.	Issuance Description	FERC Issuance Date
RD24-5-000; RD24-1-000	Notice Granting Extension of Time FERC issued a letter order granting NERC's request for additional time for filing the Petition for Approval of EOP-012-3 from March 27, 2025, to April 14, 2025.	3/26/2025

ANTICIPATED UPCOMING FILINGS

FERC Docket No.	Filing Description	Anticipated Filing Date
RM25-3-000	Reply Comments to PRC-029 NOPR	4/18/2025
TBD	Petition for approval of EOP-012-3	4/14/2025
RM24-8-000	Errata to Petition for Approval of Critical Infrastructure Protection Reliability Standards	4/29/2025
RR23-4-000	Compliance Filing Regarding Standards Rules Of Procedure Updates	5/28/2025

Standards Committee Expectations

Approved by Standards Committee January 22, 2025

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:

> *The Standards Committee (the Committee) of the North American Electric Reliability Corporation (NERC), working with NERC Standards Staff, manages and executes the Reliability Standards development process to timely develop and maintain a comprehensive set of results-based Reliability Standards.*
>
> *Section 306 of the Rules of Procedure establishes that "The Standards Committee shall provide oversight of the Reliability Standards development process to ensure stakeholder interests are fairly represented. The Standards Committee shall not under any circumstance change the substance of a draft or approved Reliability Standard."*
>
> *The Committee is responsible for ensuring that the Reliability Standards, definitions, Variances and Interpretations developed by drafting teams are developed in accordance with the processes in the Standard Processes Manual, Appendix 3A of the NERC Rules of Procedure to support NERC's benchmarks for Reliability Standards as well as criteria for governmental approval.*
>
> *The Standards Committee, as a process oversight committee, does not base its process decisions on the technical content of Reliability Standards or Standards Authorization Requests.*

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, may designate a proxy. Proxies may attend and vote at Committee meetings provided the

absent Committee member notifies in writing the Committee chair, vice chair or secretary along with the reason(s) for the proxy. SC business cannot be conducted in the absence of 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.
6. SC members should conduct themselves as detailed in the NERC Antitrust Compliance Guidelines and NERC Participant Conduct Policy.

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 cannot 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.

Decorum Talking Points

Standards Committee Meetings use the following Governance Structure:

- Following each Agenda item, the Chair will call for the Sponsor to make a presentation.
- The Chair will solicit any motions from the Committee, including motions for action on the agenda item.
- To make a motion, a member of the Standards Committee or recognized proxy must obtain the floor. To obtain the floor a member may raise their hand virtually, or table tent for in person meetings. The Chair will recognize the member, who may then state their motion.
- The motion must receive a second to be considered. To second a motion, a member would obtain the floor and state that they second the motion.
- After a second, the Chair will ask whether there is any discussion.
- At this time, SC members may either debate the motion or make another motion.
- To participate in discussion, members must obtain the floor.
- Following such discussion, the Chair will call the vote.
- To amend a motion or make another motion, a member must obtain the floor and propose their amendment. The amendment must then be seconded. The amendment must be voted on prior to returning to the main motion.
- Agenda items will pass with a simple majority of votes cast being in the affirmative. An exception exists for revisions to the Standard Processes Manual and the Standards Committee Charter, which require a 2/3 affirmative vote.