NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

December 13, 2023 | 10:00 a.m.—3:00 p.m. Eastern

NERC – Atlanta
Conference Room 612
3353 Peachtree Road N.E., Suite 600 – North Tower
Atlanta, GA 30326

Dial-in: 1-415-655-0002 | Access Code: 2308 704 2598 | Meeting Password: 121323
Click here to Join WebEx

Introduction and Chair's Remarks

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

Agenda Items

1. **Review December 13, 2023 Agenda - Approve - *Amy Casuscelli* (1 minute)**
2. **Consent Agenda - Approve - *Amy Casuscelli* (5 minutes)**
   a. November 15, 2023 Standards Committee Meeting Minutes* - **Approve**
   b. 2023 Standard Committee Accomplishments* - **Endorse**
   c. 2024 - 2026 Standards Committee Strategic Work Plan* - **Approve**
   d. 2024- 2025 Term Elections - **Inform**
3. **Projects Under Development - Review**
   a. Project Tracking Spreadsheet - *Mike Brytowski* (10 minutes)
   b. Three-Month Outlook* - *Latrice Harkness* (5 minutes)
   c. Projected Posting Schedule - *Latrice Harkness* (5 minutes)
   d. Fast Track Project - Soo Jin Kim (10 minutes)
4. **Transmission Planning Energy Scenarios Standard Authorization Request - Accept/Authorize/Authorize - *Jamie Calderon (10 minutes)***
   a. Transmission Planning Energy Scenarios Standard Authorization Request*
   b. Transmission Planning Energy Scenarios Technical Justification*
5. **Risk Management for Third-Party Cloud Services Standard Authorization Request - Accept/Authorize/Authorize - *Alison Oswald (10 minutes)***

a. Risk Management for Third-Party Cloud Services Standard Authorization Request*

6. **Project 2023-05 Modifications to FAC-001 and FAC-002* NON-PUBLIC - Appoint -** ***Jamie Calderon (10 minutes)***
7. **Project 2021-03 CIP-002* NON-PUBLIC - Appoint -** ***Alison Oswald (10 minutes)***
8. **Project 2020-02 Modifications to PRC-024 (Generator Ride-through) Waiver - Approve -** ***Jamie Calderon (10 minutes)***
9. **Project 2023-02 Analysis and Mitigation of BES Inverter-Based Resources Performance Issues Waiver - Approve -** ***Jamie Calderon (10 minutes)***
10. **Project 2021-04 Modifications to Disturbance Monitoring and Reporting Requirements Waiver - Approve -** ***Jamie Calderon (10 minutes)***
11. **Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather Waiver -** ***Jamie Calderon (10 minutes)***
12. **Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination Waiver -** ***Jamie Calderon (10 minutes)***
13. **Project 2023-03 Internal Network Security Monitoring - Authorize -** ***Alison Oswald (10 minutes)***
    a. CIP-007-X*
    b. Implementation Plan*
14. **Standards Committee Charter Revisions - Approve -** ***Amy Casuscelli (10 minutes)***
    a. Standards Committee Charter*
15. **2024 Standards Committee Executive Committee Elections* - Inform -** ***Alison Oswald (5 minutes)***
16. **SPSEG Recommendations Work Plan* - Inform -** ***Amy Casuscelli (10 minutes)***
17. **Subcommittee Updates**
    a. Project Management and Oversight Subcommittee (PMOS) - *Mike Brytowski* (10 minutes)
    b. Standards Committee Process Subcommittee (SCPS) - *Troy Brumfield* (10 minutes)
    c. Standing Committees Coordinating Group (SCCG) - *Todd Bennett* (10 minutes)
    d. Reliability and Security Technical Committee (RSTC) - *Venona Greaff* (10 minutes)
    e. NERC Board of Trustees - *Sue Kelly* (10 minutes)
18. **Legal Update and Upcoming Standards Filings - Review -** ***Sarah Crawford*** **(5 minutes)**
19. **Informational Items - Enclosed**
    a. Standards Committee Expectations*
    b. 2024 SC Meeting Schedule
    c. 2024 Standards Committee Roster
    d. Highlights of Parliamentary Procedure*

20. Adjournment

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Meeting Notice

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

Conference call/webinar version:

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

Face-to-face meeting version:

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

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

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

Minutes
Standards Committee Meeting

November 15, 2023 | 1:00—3:00 p.m. Eastern

A. Casuscelli, chair, called to order the Standards Committee (SC) meeting on November 15, 2023 at 10:00 a.m. Eastern. D. Love called roll and determined the meeting had a quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement

D. Love 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

A. Casuscelli welcomed the SC, guests, and proxies to the meeting. A. Casuscelli also reminded the committee members that the December SC meeting will be held in person in Atlanta, GA. She notified the committee that the 2024-2025 term elections concluded on November 10, 2023 and congratulated those serving on the committee in 2024. Sue Kelly gave an overview of the Reliability Conference held at FERC the previous week.

Review November 15, 2023 Agenda (agenda item 1)

The SC approved the November 15, 2023 meeting agenda.

Consent Agenda (agenda item 2)

The SC approved the September 20, 2023 and October 18, 2023 Standards Committee Meeting Minutes. S Rueckert abstained.

Projects Under Development (agenda item 3)

S. Kim provided an overview of the new standards development project prioritization. The slides will be posted on the NERC website following this meeting. M. Brytowski provided an overview. L. Harkness provided an overview.

Transmission Planning Energy Scenarios Standard Authorization Request (agenda item 4)

J. Calderon provided an overview. M. Jones asked about the informal comment process this SAR has already undergone. J. Calderon stated that was an RSTC process, not a standards comment period. S. Rueckert asked if this was assigned to Project 2023-07, whether it would be addressed as a phase 2, and whether that should be added to the SC's requested action. L. Harkness noted that the phases would be clarified on the project page, and having it in action is unnecessary. C. Yeung asked if this is a new process for the RSTC to post a SAR for comment, to which J. Calderon replied yes. C. Yeung asked what industry could do if they felt their remarks needed to be addressed by the RSTC process. L. Harkness stated she does not want this standards process mixed with the RSTC process. This SAR would still be posted for

comment like all other SARs presented to the SC. P. Winston made a motion to defer consideration of the SAR to the December meeting.

The committee approved the motion. S. Rueckert opposed, and R. Shu abstained.

Project 2020-06 Verification of Models and Data for Generators (agenda item 6)
J. Calderon provided an overview. K. Feliks asked if any outreach will be done to explain how these definitions work with the newly proposed GO/GOP-IBR concepts/registration. J. Calderon responded that these definitions are to clearly put language around the technology itself and not the registration. M. Jones asked if the original SAR, which did not indicate "add or modify glossary terms," allows this team the basis to propose these definitions. J. Calderon stated that this approach is needed to have consistency across all the IBR-related projects, and from a procedure standpoint, there is no issue. P. Winston motioned to authorize the initial posting of proposed definitions for Inverter-Based Resource (IBR) and IBR Unit that would be included in the Glossary of Terms for a 45-day formal comment period, with ballot pools formed in the first 30 days.

The committee approved the motion with no objections or abstentions.

Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather (agenda item 5)
A. Oswald provided an overview. M. Hostler asked why this project was separate from the other SAR presented earlier in the meeting. S. Kim stated that this SAR is from FERC directive 896, and before that order came out, NERC was already working on a SAR about extreme events. Due to the FERC order coming out, we moved forward with the original SAR because it has a deadline. The previous SAR would be assigned to this team to work on phase 2 of the project. V. O'Leary motioned to authorize drafting new or modified Reliability Standard(s) as identified in the Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather Standards Authorization Request (SAR).

The committee approved the motion with no objections or abstentions.

Legal Update and Upcoming Standards Filings (agenda item 7)
S. Crawford provided an update.

Adjournment
The meeting adjourned at 2:44 p.m. Eastern.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Committee 2023 Segment Representatives

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Chair 2022-23	Amy Casuscelli* Manager, Reliability Assurance & Risk Management	Xcel Energy		X
Vice Chair 2022-23	Todd Bennett* Managing Director, Reliability Compliance & Audit Services	Associated Electric Cooperative, Inc.		X
Segment 1-2022-23	Michael Jones Manager, Reliability Standards & Policy	National Grid		X
Segment 1-2023-24	Troy Brumfield* Regulatory Compliance Manager	American Transmission Company		X
Segment 2-2022-23	Jamie Johnson Infrastructure Compliance Manager	California ISO		X
Segment 2-2022-23	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool		X
Segment 3-2022-23	Kent Feliks Manager NERC Reliability Assurance – Strategic Initiatives	American Electric Power Company, Inc.		X
Segment 3-2023-24	Vicki O' Leary Director – Reliability, Compliance, and Implementation	Eversource Energy		X
Segment 4-2022-23	Marty Hostler Reliability Compliance Manager	Northern California Power Agency		X
Segment 4-2023-24	Patti Metro Senior Grid Operations & Reliability Director	National Rural Electric Cooperative Associate		X
Segment 5-2022-23	Terri Pyle Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric		X
Segment 5-2023-24	Jim Howell Markets Compliance Manager	Southern Company Generation		X

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Segment 6-2022-23	Sarah Snow* Manager of Reliability Compliance	Cooperative Energy		X
Segment 6-2023-24	Justin Welty Senior Manager, NERC Reliability Standards	NextEra Energy		X
Segment 7-2022-23	Kristine Martz Industry Specialist, Power & Utilities	Amazon Web Services		X
Segment 7-2023-24	Venona Greaff* Senior Energy Analyst	Occidental Chemical Corporation		X
Segment 8-2022-23	Robert Blohm[1] Managing Director	Keen Resources Ltd.		X
Segment 8-2023-24	Philip Winston Retired (Southern Company)	Independent		X
Segment 9-2022-23	Sarosh Muncherji[1] Cyber Security Specialist	British Columbia Utilities Commission	Nicole Manalili	X
Segment 9-2023-24	William Chambliss General Counsel	Virginia State Corporation Commission		X
Segment 10-2022-23	Tony Purgar Senior Manager, Operational Analysis & Awareness	ReliabilityFirst		X
Segment 10-2023-24	Steven Rueckert Director of Standards	WECC		X

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

2023 Standards Committee Accomplishments

Action

Endorse the following Standards Committee Executive Committee (SCEC) determination on the Standards Committee (SC) 2023 accomplishments:

Focus Area: Process Improvement

- Implement Board Recommended Enhancements to the Reliability Standards Development Process from the Stakeholder Engagement Group – Completed

  The SC Chair and Vice Chair led an initiative to implement the Board of Trustee recommendations specific to the SC to enhance the standards development process through close coordination with NERC staff, other standing committees, and the Standing Committee Coordinating Group (SCCG).

- Standards Grading – Completed

  The SC and the Compliance and Certification Committee formed a joint task force in early 2023 to evaluate the existing Standards Grading process, identify opportunities, and provide recommendations for improvement. This work continues into 2024 and was completed in lieu of the annual Standards Grading exercise.

Focus Area: Risk Mitigation

- Standards Development Prioritization - Completed

  In support of the recommendations of the Stakeholder Engagement Group, the SC partnered with NERC staff and the SCCG to prioritize standards development projects effectively based on reliability risk.

- ERO Risk Framework - Completed

  Executed and built on the role of the SC in the framework, which includes active participation in the SCCG and framework identified feedback loops.

Focus Area: Standards Quality

- FERC Directives - Completed

  As detailed in the 2023-2025 Reliability Standards Development Plan, two outstanding FERC directives are being resolved through the development process. The SC has monitored progress and is supportive of the final resolution of these directives through the completion of the following projects:

  - Project 2016-02 Modifications to CIP Standards
  - Project 2020-04 Modifications to CIP-012

- Periodic Reviews - Delayed

  The Project Management and Oversight Subcommittee (PMOS) periodic review project was placed on hold to more closely align with the Standards Grading task force

initiative. With 25 open standards projects, this aligns with lower project priority criteria for NERC.

- Transition of Guidelines and Technical Basis to Technical Rationale – Ongoing

  The SC continued to review Guidelines and Technical Basis documents for transition to Technical Rationale documents as well as moving compliance examples contained in open Standards projects to Implementation Guidance.

Background

The SCEC reviews each of the annual required tasks and provides the results of whether the SC accomplished each required task at the December meeting. Consistent with the SC Strategic Work Plan review at the end of 2022, the SCEC uses a binary self-evaluation process to assess the accomplishments and presents the results of each assigned task for the SC's endorsement. The SCEC agreed on the above evaluations.

2024-2026 Standards Committee Strategic Work Plan

Introduction

The Standards Committee (SC) Strategic Work Plan (Plan) focuses SC actions on overseeing Standards development activities, including:

- Addressing emerging risks using input from various sources, including the Reliability and Security Technical Committee (RSTC) and the Reliability Issues Steering Committee (RISC)
- Prioritizing standards development activities
- Supporting process improvements to enhance agility and effectiveness
- Addressing Federal Energy Regulatory Commission (FERC) directives

Emerging Risks

Through input by a NERC technical committee, the RISC, or a governmental authority (such as FERC), the SC authorizes the development of new or revised standards to mitigate emergent risks, as appropriate.

Vision, Mission, and Guiding Principles

Vision

A comprehensive body of results-based Reliability Standards focused on minimizing risk to the North American bulk power system (BPS).

Mission

The SC is a ballot body elected stakeholder Committee serving and reporting directly to the NERC Board of Trustees (Board). The SC partners with NERC staff to manage and oversee development of a comprehensive set of results-based Reliability Standards prioritized and focused on risk to the bulk power system while maintaining attributes of due process, openness, and balance of interests.

Guiding Principles

- Promote and implement a collaborative working environment with other NERC Standing Committees, NERC Standards staff, stakeholders, and standard drafting teams.
- Execute the Standards development process openly and inclusively for effective and efficient use of NERC and industry resources.
- Promote and take a leadership role on consensus-building activities.

Work Plan

Consistent with the 2023-2025 Reliability Standards Development Plan (RSDP), this Plan recognizes the transition of the Standard development process to primarily address a small number of FERC directives,

emerging risks, and process improvements. The details of the goals and objectives for 2024-2026 appear in the RSDP.

Focus Area: Process Improvement

To promote continuous improvement, existing processes must be periodically reviewed. In support of the vision, mission, and guiding principles above, the SC will undertake certain actions.

Monitor Implementation of Board Recommended Enhancements to the Reliability Standards Development Process from the Stakeholder Engagement Group

- The SC Chair and Vice Chair led an initiative in 2023 to implement the Board of Trustee recommendations specific to the SC to enhance the standards development process. Implementation of these recommendations, requiring SC coordination with NERC Staff, other standing committees, and the Standing Committee Coordinating Group (SCCG), is complete. The SC leadership will monitor the effective deployment of the recommendations.

Standards Grading

- In 2023 the SC and the Compliance and Certification Committee convened a joint task force to evaluate the existing Standards Grading process, identify opportunities, and provide recommendations for improvement. This review occurred in lieu of the annual Standards Grading exercise. The task force's work is still ongoing and will reconvene in early 2024.

Focus Area: Risk Mitigation

To develop a comprehensive body of risk and results-based Reliability Standards, the SC will focus on the activities below:

Standards Development Prioritization

- In support of the recommendations of the Stakeholder Engagement Group, the SC will partner with NERC Staff and consult with the SCCG to prioritize standards development projects based on reliability risk effectively.

Risk Framework

- Continue to execute and build on the role of the SC in the NERC Risk Mitigation Framework, which includes active participation in the SCCG identified opportunities for feedback loops.

Focus Area: Standards Quality

The Reliability Standards should be clearly written, effective in mitigating risk to the BPS, and not unnecessarily administratively burdensome. To ensure the highest quality body of Standards, the SC will focus on the following:

FERC Directives

- As detailed in the 2024-2026 Reliability Standards Development Plan, there are eleven outstanding FERC directives being resolved through the Development process. The SC will

continue to monitor progress and support final resolution of these directives, as well as any future work related to directives.

Periodic Reviews

- The Project Management and Oversight Subcommittee (PMOS) and NERC staff will identify and schedule Periodic Reviews for SC endorsement. The PMOS will use the most recent Standards Grading results to prioritize/schedule by the end of 1st quarter 2023.

Transition of Guidelines and Technical Basis to Technical Rationale

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

3 Month Outlook

December	
Accept/Authorize SAR - SC Action	**Posting Information**
Transmission Planning Energy Scenarios	Low priority, no posting until Phase 1, order 896, completed
Risk Management for Third-Party Cloud Services	Low priority, no posting in first half of 2024
Request Waivers for Postings - SC Action	
2020-02 Modifications to PRC-024 (Generator Ride-through)	No posting associated at this time
2023-02 Analysis and Mitigation of BES Inverter-Based Resources Performance Issues	No posting associated at this time
2021-04 Modifications to Disturbance Monitoring and Reporting Requirements	No posting associated at this time
2023-07 Transmission System Planning Performance Requirements for Extreme Weather	No posting associated at this time
2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination	**January 2024**
Authorize Initial Posting - SC Action	
2023-03 Internal Network Security Monitoring (INSM)	**Week of December 11**
Final Ballot Postings	
2022-01 Reporting ACE Definition and Associated Terms	**Week of December 11**
January	
Authorize Initial Posting - SC Action	
2022-03 Energy Assurance with Energy-Constrained Resources	**Week of January 22**
Additional Ballot Postings	
2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination	TBD
February	
Authorize Initial Posting - SC Action	
2023-07 Transmission System Planning Performance Requirements for Extreme Weather	TBD
2020-02 Modifications to PRC-024 (Generator Ride-through)	TBD
2023-02 Performance of IBRs	TBD
Additionall Ballot Postings	
2021-04 Modifications to PRC-002-2	TBD

Transmission Planning Energy Scenarios

Action

- Accept the Transmission Planning Energy Scenarios Standard Authorization Request (SAR) submitted by the NERC and Regional Entities representing each interconnection;
- Authorize posting of the SAR for a 30-day formal comment period; and
- Authorize solicitation of a drafting team (DT).

Background

The *2023 ERO Reliability Risk Priorities Report*[1] defines and prioritizes risks to the reliable performance of the bulk power system (BPS). The report highlighted the need to consider three transmission planning energy-related scenarios to mitigate risks to the BPS. To address these risks, NERC included in its 2023 Work Plan Priorities the submission of a SAR to the Standards Committee (SC). The NERC Board of Trustees approved NERC's work plan priorities during its November 16, 2022 meeting.[2] The objective of the SAR is to complement the TPL-001-5.1[3] NERC Reliability Standard with the creation of one or more new Reliability Standard(s) that require energy-related transmission planning scenarios that address risks posed by

- Normal and extreme natural events,[4]
- Natural gas/electricity interdependencies, and
- Distributed Energy Resource (DER) events.

The ERO Enterprise technical staff prepared the SAR and the accompanying technical justification document for the Transmission Planning Energy Scenarios. Both documents were posted for a 30-day and a 45-day informal comment period, which resulted in substantial revisions to the SAR and justification. Refer to the Quick Reference Guide[5] for additional information and links to the posting documents, redlines, and responses to comments.

Summary

NERC staff recommends that the SC accept SAR, authorize posting of the SAR for a 30-day formal comment period, and solicitation of a DT. Standards staff plan to initiate the project upon substantially completing Project 2023-07 – Extreme Heat and Cold Weather.

---

[1] https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf

[2] https://www.nerc.com/AboutNERC/StrategicDocuments/2023_NERC_Work_Plan_Priorities_Board_Approved_November_16_2022.pdf

[3] TPL-001-5.1 – Transmission System Planning Performance Requirements available at: https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-5.1.pdf.

[4] Extreme heat and cold weather events are being addressed by NERC Project 2023-07 in response to FERC Docket RM22-10-000, Order No. 896, document number 2023-13286 at https://www.federalregister.gov/documents/2023/06/23/2023-13286/transmission-system-planning-performance-requirements-for-extreme-weather.

[5] https://www.nerc.com/pa/Documents/QuickReferenceGuide_EnergyScenarios.pdf.

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Transmission Planning Energy Scenarios		
Date Submitted:	October 30, 2023		
SAR Requester			
Name:	Scott Barfield-McGinnis, NERC, Principal Technical Advisor, Power Risk Issues and Strategic Management Enoch Davies, Western Electricity Coordinating Council, Manager, Reliability Modeling Neeraj Lal, Northeast Power Coordinating Council, Manager, System Studies Mohamed Osman, NERC, Lead Engineer of System Analysis, Power System Analysis Dianlong Wang, Midwest Reliability Organization, Senior Power System Engineer Brad Woods, Texas RE, Senior Reliability Engineer		
Organization:	NERC and the six Regional Entities		
Telephone:	Scott: 404-446-9689 Enoch: 801-883-6860 Neeraj: 917-934-7969 Mohamed: 404-446-9634 Dianlong: 651-855-1751 Brad: 512-583-4957	Email:	Scott.Barfield@nerc.net enoch@wecc.org nlal@npcc.org Mohamed.Osman@nerc.net dianlong.wang@mro.net brad.woods@texasre.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	

Requested information
What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The current transmission planning Reliability Standard TPL-001-5.1 – Transmission System Planning Performance Requirements[1] does not expressly require transmission planners and planning coordinators to consider in the long-term planning horizon (1) normal and extreme natural events,[2] (2) gas-electric interdependencies and (3) distributed energy resources (DER) events. In particular, Reliability Standard TPL–001–5.1, Table 1, provisions 3. b (steady state) and 2. j (stability) require analyses to be performed for certain events based upon operating experience but do not expressly require these three types of impacts.

Events related to these three areas have spanned the continent in recent years and demonstrate the challenges associated with planning, particularly those events that affect a wide area or that occur during periods when the Bulk-Power System (BPS) must meet unexpectedly high demand. Extreme weather events have occurred with greater frequency in recent years and are projected to occur with even greater frequency in the future. Dependency on natural gas is increasing as it is becoming a more significant share of the dispatchable resources due to large thermal plant retirements and increases in renewables. Lastly, DER has been and continues to be, an area that has been shown to create impacts on the BPS planning as well as its operation.

Events have shown that the risk of such events can pose to the reliable operation of the BPS and is accentuated by the FERC Order No. 896[3] ("Order") directing NERC to require transmission system planning for extreme heat and cold weather events that impact the Reliable Operation of the BPS. The Order emphasizes that long-term transmission planning, along with other measures, can play an important role in identifying and helping to minimize not only extreme heat and cold weather events but also the three risks noted above.

In parallel with the efforts related to the Order and in addition to the priorities identified in NERC's work plan priorities informed by the Reliability Issues Steering Committee (RISC), this project will similarly harmonize the NERC TPL-001 transmission planning Reliability Standard with the creation of one or more new Reliability Standard(s) to address (1) normal and extreme natural events, (2) gas-electric interdependencies, and (3) DER. The potential risks for cascading outages that may be caused by these three areas of risk should use benchmark events[4] and planning cases[5], have both the steady-state and stability analyses conducted, and have corrective action plans developed and implemented where BPS performance cannot be met.

[1] TPL-001-5.1 at https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-5.1.pdf.
[2] Normal and extreme natural events will not include extreme heat and cold as addressed in the FERC Order No. 896.
[3] Order No. 896, *Transmission System Planning Performance Requirements for Extreme Weather*, 183 FERC ¶ 61,191 (2023), available at https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230615-3100&optimized=false.
[4] The transmission planning analyses intend to target specific cases called benchmark events for which energy scenarios would be applied according to defined performance criteria.
[5] Power flow cases used in performing transmission planning studies.

Requested information
The modification of the Reliability Standard(s) will establish benchmark events related to the three risk areas[6] for required analyses and require the development of planning cases with appropriate sensitivities over a wide area. The Reliability Standard(s) must require the identification and implementation of corrective actions where system performance requirements are not met, including appropriate coordination and communication of studies.
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?):
The purpose of this project is to address the transmission planning reliability gaps that do not expressly require transmission planners and planning coordinators to consider (1) normal and extreme weather, (2) gas-electric interdependencies, and (3) DER in their transmission planning assessments in the long-term planning horizon. Using the Transmission Planning Energy Scenarios Technical Justification Document, October 2023 ("White Paper"), the goal in revising an existing Reliability Standard(s) or creating one or more new Reliability Standard(s) is to: A. Revise the TPL Reliability Standard and/or develop one or more new Reliability Standard(s) (addressing all three risk areas). B. Develop energy scenario-based[7] benchmark events and planning cases. C. Consider defining "wide area" if needed to address defined energy scenarios.[8] D. Identify responsible functional entities for developing benchmark events and planning cases and for conducting studies over a wide area. E. Require coordination among responsible entities and the sharing of data and studies. F. Require study of concurrent/correlated generator and transmission outages. G. Conduct transmission system planning studies of all three risk areas over the long-term planning horizon, including: a. Steady state and transient stability analyses. b. Sensitivity analysis applying appropriate sensitivities based on collaboration from neighboring planners. c. Consider modification to the traditional planning approach(es). H. Require the development of corrective action plans that mitigate specified instances where performance requirements are not met. I. Establish an appropriate implementation timeline to address the risks.
Project Scope (Define the parameters of the proposed project):
The scope of the proposed project is to develop one or more new transmission planning Reliability Standard(s) or modify an existing Reliability Standard to address the issues and criteria discussed in

[6] Risk areas: (1) Normal and extreme weather, (2) gas-electric interdependencies, and (3) distributed energy resources (DER).
[7] E.g., Energy scenarios including, but not limited to traditional or normal patterns (i.e., "de-carbonization and policy", significant changes in alternative generation resources (i.e., "high renewables penetration"), and induced increases in consumption due to electrifications (i.e., "high demand").
[8] Wide Area is defined in Glossary of Terms Used in NERC Reliability Standards. The subject matter experts charged with defining "wide area" will need to consider revising the defined term of creating a different term.

Requested information
the White Paper in collaboration with those efforts to address directives from FERC Order No. 896 pertaining to the study of extreme heat and cold weather events. New or revised definitions may be required (e.g., "wide area"). This project may also need to revise Reliability Standard MOD-032-1 – Data for Power System Modeling and Analysis[9] for data sharing.
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[10] for developing a new or revised Reliability Standard or definition, which includes a discussion of the risk and impact on the reliability of the BES, and (2) a technical foundation document (*e.g.,* research paper) to guide the development of the Standard or definition):
The individuals responsible for the development of one or more new Reliability Standard(s) or the modification of a Reliability Standard shall achieve the actions listed below related to addressing the three identified risk areas pertaining to transmission system planning over the long-term planning horizon that impact the Reliable Operation of the BPS. The technical justification and foundation of the reliability-related benefits is addressed in the White Paper concerning the developing of one or more new Reliability Standard(s) and/or modifying an existing Reliability Standard, which includes the addition or modification of any term(s) used in Reliability Standards. To assist the drafting team for this project and those efforts addressing Order No. 896 directives, the following actions have been prepared in a sequence consistent with the directives in the Order. **Normal Natural Events** A. Revise to harmonize the TPL-001-5.1 Reliability Standard and/or develop one or more new Reliability Standard(s) to address normal natural events. B. Develop energy scenario-based benchmark planning event and planning cases that include addressing: a. Seasonal demand variations. b. Planned energy resource additions. c. Resource variability. d. Factors that affect the scope of energy scenarios: i. Identifying geographical regional differences in climate and weather patterns. ii. Using historical natural event meteorological data from reliable sources (e.g., national laboratories, regional transmission operators (RTO), National Oceanic

[9] See MOD-032-1 at https://www.nerc.com/pa/Stand/Reliability%20Standards/MOD-032-1.pdf.

[10] 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

and Atmospheric Administration (NOAA), Environment Canada, and other local, state, and federal agencies and organizations.

iii. Applying a common method to follow when creating benchmark planning cases.

iv. Potential event-related coincident contingencies (e.g., concurrent/correlated generation and transmission outages, derates, etc.) and expected future conditions of the system, such as changes in load.

v. Available transfers.

vi. Generation resource mix.

vii. Identifying facilities sensitive to certain events.

C. Consider defining "wide area" if needed to address defined energy scenarios.

D. Identify responsible functional entities for developing:

a. Benchmark events.

b. Planning cases.

c. Entities to conduct studies over a wide area.

d. Corrective action plans.

E. Require coordination among responsible entities and the sharing of data and studies.

F. Require the study of concurrent/correlated generator and transmission outages.

G. Conduct transmission system planning studies for normal, natural events over the long-term planning horizon for:

a. Steady-state analyses – The steady-state analyses need to assess the system performance under no contingencies (e.g., P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Steady-state studies must:

i. Apply normal natural weather benchmark planning events to the planning case.

ii. Apply the defined energy scenarios to each benchmark planning event.

iii. Include specific defined criteria for determining concurrent and correlated outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

b. Transient stability analyses – The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies, but not

Requested information

necessarily mirroring or to the rigor of the TPL-001 Reliability Standard planning contingencies (e.g., Categories P1-P7). Stability studies must:

i. Apply normal, natural event benchmark planning events.

ii. Apply the defined energy scenario contingencies (e.g., high demand and low resource availability) to each benchmark planning event.

iii. Include specific defined criteria for determining concurrent and correlated unplanned outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

c. Sensitivity analysis applying appropriate sensitivities based on collaboration from neighboring planners. The following are minimum considerations:

i. Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark planning case.

ii. Establish a baseline set of sensitivities that include conditions that vary with temperature, such as load, generation, and system transfers.

iii. Document sensitivity assumptions.

d. Consider modification to the traditional planning approach(es). Consider the following probabilistic approaches at a minimum:

i. Whether probabilistic techniques can be incorporated into the new or modified Reliability Standard(s) and implemented by responsible entities and

ii. If a probabilistic approach is feasible and reasonable, address factors such as:

1. A projected frequency (e.g., 1-in-50-year event), or

2. A probability distribution (95th percentile event).

H. Require the development of corrective action plans that mitigate specified instances where performance requirements are not met. Corrective action plans must:

a. Identify specified instances in benchmark event cases when performance standards are not met.

b. Establish required study contingencies and baseline sensitivities for which a corrective action plan is required.

c. Determine whether corrective action plans should be required for single or multiple sensitivity cases.

Requested information

d. Determine whether corrective action plans should be developed if a benchmark event that is not already included in benchmark planning case would result in cascading outages, uncontrolled separation, or instability.

e. Require mitigation for specified instances where performance requirements for benchmark events and energy scenarios are not met (*i.e.* when certain benchmark studies conducted under the Reliability Standard show that a benchmark event would result in cascading outages, uncontrolled separation, or instability).

f. Require certain processes to facilitate interaction and coordination with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service, as appropriate in implementing a corrective action plan.

g. Require that responsible entities share their corrective action plans with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service issues.

I. Establish an appropriate implementation timeline to address the risks.

J. Establish a method and interval (e.g., every 3-5 years) for periodic updates to benchmark event and planning cases, inputs, energy scenarios, assumptions, and other key data required to conduct studies.

Extreme Natural Events

A. Revise to harmonize the TPL-001-5.1 Reliability Standard and/or develop one or more new Reliability Standard(s) to address extreme natural events.

B. Develop energy scenario-based benchmark planning event and planning cases that include addressing:

a. Seasonal demand variations.

b. Planned energy resource additions.

c. Resource variability.

d. Factors that affect the scope of energy scenarios:

i. Identifying geographical regional differences in climate and weather patterns.

ii. Using extreme natural event meteorological data from reliable sources (e.g., national laboratories, regional transmission operators (RTO), National Oceanic and Atmospheric Administration (NOAA), Environment Canada, and other local, state, and federal agencies and organizations.

iii. Applying a common method to follow when creating benchmark planning cases.

Requested information

iv. Potential event-related coincident contingencies (e.g., concurrent/correlated generation and transmission outages, derates, etc.) and expected future conditions of the system, such as changes in load.

v. Available transfers.

vi. Generation resource mix.

vii. Identifying facilities sensitive to certain events.

C. Consider defining "wide area" if needed to address defined energy scenarios.

D. Identify responsible functional entities for developing:

a. Benchmark events.

b. Planning cases.

a. Entities to conduct studies over a wide area.

c. Corrective action plans.

E. Require coordination among responsible entities and the sharing of data and studies.

F. Require the study of concurrent/correlated generator and transmission outages.

G. Conduct transmission system planning studies for extreme natural events over the long-term planning horizon for:

a. Steady-state analyses – The steady-state analyses need to assess the system performance under no contingencies (e.g., P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Steady-state studies must:

i. Apply extreme natural weather benchmark planning events to the planning case.

ii. Apply the defined energy scenarios to each benchmark planning event.

iii. Include specific defined criteria for determining concurrent and correlated outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

b. Transient stability analyses – The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies, but not necessarily mirroring or to the rigor of the TPL-001 Reliability Standard planning contingencies (e.g., Categories P1-P7). Stability studies must:

i. Apply extreme natural event benchmark planning events.

Requested information

ii. Apply the defined energy scenario contingencies (e.g., high demand and low resource availability) to each benchmark planning event.

iii. Include specific defined criteria for determining concurrent and correlated unplanned outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

c. Sensitivity analysis applying appropriate sensitivities based on collaboration from neighboring planners. The following are minimum considerations:

i. Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark planning case.

ii. Establish a baseline set of sensitivities that include conditions that vary with temperature, such as load, generation, and system transfers.

iii. Document sensitivity assumptions.

d. Consider modification to the traditional planning approach(es). Consider the following probabilistic approaches at a minimum:

i. Whether probabilistic techniques can be incorporated into the new or modified Reliability Standard(s) and implemented by responsible entities and

ii. If a probabilistic approach is feasible and reasonable, address factors such as:

1. A projected frequency (e.g., 1-in-50-year event), or

2. A probability distribution (95th percentile event).

H. Require the development of corrective action plans that mitigate specified instances where performance requirements are not met. Corrective action plans must:

a. Identify specified instances in benchmark event cases when performance standards are not met.

b. Establish required study contingencies and baseline sensitivities for which a corrective action plan is required.

c. Determine whether corrective action plans should be required for single or multiple sensitivity cases.

d. Determine whether corrective action plans should be developed if a benchmark event that is not already included in benchmark planning case would result in cascading outages, uncontrolled separation, or instability.

Requested information

e. Require mitigation for specified instances where performance requirements for benchmark events and energy scenarios are not met (*i.e.* when certain benchmark studies conducted under the Reliability Standard show that a benchmark event would result in cascading outages, uncontrolled separation, or instability).

f. Require certain processes to facilitate interaction and coordination with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service, as appropriate in implementing a corrective action plan.

g. Require that responsible entities share their corrective action plans with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service issues.

I. Establish an appropriate implementation timeline to address the risks.

J. Establish a method and interval (e.g., every 3-5 years) for periodic updates to benchmark event and planning cases, inputs, energy scenarios, assumptions, and other key data required to conduct studies.

Natural Gas Interdependencies

A. Revise to harmonize the TPL-001-5.1 Reliability Standard and/or develop one or more new Reliability Standard(s) to address natural gas interdependencies.

B. Develop energy scenario-based benchmark planning event and planning cases that include addressing:

   a. Gas supply disruptions.

   b. Electric power supply disruptions.

   c. Fuel switching.

   d. Renewable energy integration.

C. Consider defining "wide area" if needed to address defined energy scenarios.

D. Identify responsible functional entities for developing:

   a. Benchmark events.

   b. Planning cases.

   c. Entities to conduct studies over a wide area.

   d. Corrective action plans.

E. Require coordination among responsible entities and the sharing of data and studies.

F. Require the study of concurrent/correlated generator and transmission outages.

G. Conduct transmission system planning studies for natural gas interdependencies over the long-term planning horizon for:

   a. Steady-state analyses – The steady-state analyses need to assess the system performance under no contingencies (e.g., Category P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Steady-state studies must:

      i. Apply natural gas interdependency benchmark planning events to the planning case.

      ii. Apply the defined energy scenarios to each benchmark planning event.

      iii. Include specific criteria for determining concurrent and correlated outages of both generators and transmission lines.

      iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

      v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

Requested information

b. Transient stability analyses – The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies, but not necessarily mirroring or to the rigor of the TPL-001 Reliability Standard planning contingencies (e.g., Categories P1-P7). Stability studies must:

   i. Apply natural gas interdependency benchmark planning events.

   ii. Apply the defined energy scenario contingencies (e.g., high demand, low resource availability, fuel switching) to each benchmark planning event.

   iii. Include specific criteria for determining concurrent and correlated unplanned outages of both generators and transmission lines.

   iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

   v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

   vi. Evaluate risks of compressor stations electric motors stalling.

c. Sensitivity analysis applying appropriate sensitivities based on collaboration from neighboring planners. The following are minimum considerations:

   i. Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark planning case.

   ii. Establish a baseline set of sensitivities that include conditions that vary with temperature, such as load, generation, and system transfers.

   iii. Document sensitivity assumptions.

d. Consider modification to the traditional planning approach(es). Consider the following probabilistic approaches at a minimum:

   i. Whether probabilistic techniques can be incorporated into the new or modified Reliability Standard(s) and implemented by responsible entities and

   ii. If a probabilistic approach is feasible and reasonable, address factors such as:

      1. A projected frequency (e.g., 1-in-50-year event), or

      2. A probability distribution (95th percentile event).

H. Require the development of corrective action plans that mitigate specified instances where performance requirements are not met. Corrective action plans must:

   a. Identify specified instances in benchmark event cases when performance standards are not met.

Requested information
b. Establish required study contingencies and baseline sensitivities for which a corrective action plan is required. c. Determine whether corrective action plans should be required for single or multiple sensitivity cases. d. Determine whether corrective action plans should be developed if a benchmark event that is not already included in benchmark planning case would result in cascading outages, uncontrolled separation, or instability. e. Require mitigation for specified instances where performance requirements for benchmark events and energy scenarios are not met (*i.e.* when certain benchmark studies conducted under the Reliability Standard show that a benchmark event would result in cascading outages, uncontrolled separation, or instability). f. Require certain processes to facilitate interaction and coordination with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service, as appropriate in implementing a corrective action plan. g. Require that responsible entities share their corrective action plans with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service issues. I. Establish an appropriate implementation timeline to address the risks. J. Establish a method and interval (e.g., every 3-5 years) for periodic updates to benchmark event and planning cases, inputs, energy scenarios, assumptions, and other key data required to conduct studies.
Distributed Energy Resources A. Revise to harmonize the TPL-001-5.1 Reliability Standard and/or develop one or more new Reliability Standard(s) to address distributed energy resources (DER). B. Develop energy scenario-based benchmark planning event and planning cases that include addressing: a. High DER penetration scenarios. b. DER variability and intermittency. c. BPS support from DERs. d. DER outage scenarios. C. Consider defining “wide area” if needed to address defined energy scenarios. D. Identify responsible functional entities for developing: a. Benchmark events.

Requested information

b. Planning cases.

c. Entities to conduct studies over a wide area.

d. Corrective action plans.

E. Require coordination among responsible entities and the sharing of data and studies.

F. Require the study of concurrent/correlated generator and transmission outages.

G. Conduct transmission system planning studies for DER energy scenarios over the long-term planning horizon for:

a. Steady-state analyses – The steady-state analyses need to assess the system performance under no contingencies (e.g., P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Steady-state studies must:

i. Apply the DER benchmark planning events to the planning case.

ii. Apply the defined energy scenarios to each benchmark planning event.

iii. Include specific criteria for determining concurrent and correlated outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

b. Transient stability analyses – The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies, but not necessarily mirroring or to the rigor of the TPL-001 Reliability Standard planning contingencies (e.g., Categories P1-P7). Stability studies must:

i. Apply the DER benchmark planning events.

ii. Apply the defined energy scenario contingencies (e.g., high demand, low DER availability) to each benchmark planning event.

iii. Include specific criteria for determining concurrent and correlated unplanned outages of both generators and transmission lines.

iv. Model demand load response in benchmark planning event cases as a corrective action to meet system performance criteria.

v. Evaluate the wide area performance during such benchmark planning events and energy scenarios.

c. Sensitivity analysis applying appropriate sensitivities based on collaboration from neighboring planners. The following are minimum considerations:

Requested information

i. Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark planning case.

ii. Establish a baseline set of sensitivities that include conditions that vary with temperature, such as load, generation, and system transfers.

iii. Document sensitivity assumptions.

d. Consider modification to the traditional planning approach(es). Consider the following probabilistic approaches at a minimum:

i. Whether probabilistic techniques can be incorporated into the new or modified Reliability Standard(s) and implemented by responsible entities and

ii. If a probabilistic approach is feasible and reasonable, address factors such as:

1. A projected frequency (e.g., 1-in-50-year event), or

2. A probability distribution (95th percentile event).

H. Require the development of corrective action plans that mitigate specified instances where performance requirements are not met. Corrective action plans must:

a. Identify specified instances in benchmark event cases when performance standards are not met.

b. Establish required study contingencies and baseline sensitivities for which a corrective action plan is required.

c. Determine whether corrective action plans should be required for single or multiple sensitivity cases.

d. Determine whether corrective action plans should be developed if a benchmark event that is not already included in benchmark planning case would result in cascading outages, uncontrolled separation, or instability.

e. Require mitigation for specified instances where performance requirements for benchmark events and energy scenarios are not met (*i.e.* when certain benchmark studies conducted under the Reliability Standard show that a benchmark event would result in cascading outages, uncontrolled separation, or instability).

f. Require certain processes to facilitate interaction and coordination with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service, as appropriate in implementing a corrective action plan.

g. Require that responsible entities share their corrective action plans with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service issues.

Requested information
I. Establish an appropriate implementation timeline to address the risks. J. Establish a method and interval (e.g., every 3-5 years) for periodic updates to benchmark event and planning cases, inputs, energy scenarios, assumptions, and other key data required to conduct studies.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The cost impact is unknown and will be considered during the Reliability Standard development process. However, the SAR proposes to either create one or more new Reliability Standard(s) or modify an existing Reliability Standard that would require identified responsible entities to create corrective action plans to address risks related to transmission system planning performance for the three risk areas. The costs associated with a revised and one or more new Reliability Standard(s) are anticipated to be comparable to those associated with a responsible entity's experience in the performance of TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events for each identified risk area.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
The results of improved studies that inform mitigation needs and/or enhancements to generation and transmission based on the analyses performed by the transmission planners may uniquely impact BES facilities. For example, mitigating and corrective actions may require transmission system topology changes, including but not limited to re-evaluating load shedding plans as a safety net in response to high demand during an extreme natural weather event over a wide area. Also, if studies reveal thermal violations that could be anticipated during extreme weather, transmission facilities may need to be upgraded. Generation facilities may be impacted by having to change the way concurrent or coincident generator outages are managed and planned to reduce the likelihood of not meeting high demands over a wide area. For example, if multiple generators are disrupted due to pipeline issues and don't have dual fuel capability.
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:
Developing one or more new or modified Reliability Standard(s) should consider expertise from the following functional entities: Balancing Authority, Distribution Provider, Generator Owner, Planning Coordinator, Reliability Coordinator, Resource Planner, Transmission Owner, and Transmission Planner.

Requested information
Do you know of any consensus building activities[11] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Yes, the White Paper and this SAR was developed as an ERO Enterprise collaboration, which is comprised of technical staff from NERC and NERC's six Regional Entities. Also, in Order No. 896, FERC highlighted that industry experts agreed that extreme weather events are likely to become more severe and frequent in the future, and there is a need to address them in the long-term planning horizon.
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)?
TPL-001-5.1, MOD-032-1, and for potential coordination 2022-02 Modifications to TPL-001-5.1 and MOD-032-1,[12] Project 2022-03 Energy Assurance with Energy-Constrained Resources - Planning Horizon,[13] and Project 2022-04 EMT Modeling,[14] Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather,[15] and Project 2023-08 Modifications of MOD-031 Demand and Energy Data.[16]
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.
None.

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 an 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.

[11] 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.
[12] See: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx
[13] See: https://www.nerc.com/pa/Stand/Pages/Project2022-03EnergyAssurancewithEnergy-ConstrainedResources.aspx
[14] See: https://www.nerc.com/pa/Stand/Pages/Project2022-04EMTModeling.aspx
[15] See: https://www.nerc.com/pa/Stand/Pages/Project-2023-07-Mod-to-TPL00151.aspx
[16] See: https://www.nerc.com/pa/Stand/Pages/Project2023-08-Modifications-of-MOD-031-Demand-and-Energy-Data.aspx

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	No needed Regional or Interconnection variances were identified.

For Use by NERC Only

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

Transmission Planning Energy Scenarios

Technical Justification Document | October 2023

Introduction

The *2023 ERO Reliability Risk Priorities Report*[1] defines and prioritizes risks to the reliable performance of the bulk power system (BPS). The report highlighted the need to consider three transmission planning energy-related scenarios to mitigate risks to the BPS. To address these risks, NERC included in its 2023 Work Plan Priorities the submission of a SAR to the Standards Committee. The NERC Board of Trustees approved NERC's work plan priorities during its November 16, 2022, meeting.[2] The objective is to harmonize the NERC TPL-001-5.1[3] Reliability Standard with the creation of one or more new Reliability Standards focused on transmission planning analyses that apply energy-related scenarios that consider the following at minimum:

- Normal and extreme natural events[4]
- Natural gas/electricity interdependencies
- Distributed Energy Resource (DER) events

Cyber-informed transmission planning was considered to be a part of addressing the above three areas during the development of this technical justification. Since the ERO Enterprise (i.e., NERC and the six Regional Entities) is currently piloting the use of the Cyber-Informed Transmission Planning Framework (CITPF) with stakeholder involvement, the cyber portion of this energy scenario effort is being deferred pending the pilot results. The (CITP) *Cyber-Informed Transmission Planning Roadmap for Integrating Cyber Security into Transmission Planning Activities* [5] introduces the CITPF for including cyber security threats, particularly from coordinated attacks, into transmission planning studies that are most commonly conducted by Transmission Planners (TPs) and Planning Coordinators (PCs). The CITPF is intended to drive investments in cyber security where warranted and can be used by various entities—NERC, Regional Entities, industry stakeholders, regulators, and policymakers—to perform reliability studies; these studies will uncover unacceptable risks to the BPS that should be addressed with appropriate mitigations.

The transmission planning analyses intend to target specific cases, called "benchmark events," for which energy scenarios would be applied according to using the criteria described in each of the following energy-

[1] ERO Risk Priorities Report 2023
[2] 2023 Work Plan Priorities, slide 3.
[3] TPL-001-5.1 – Transmission System Planning Performance
[4] FERC Docket RM22-10-000, Order No. 896, document number 2023-13286 | Transmission System Planning Performance Requirements for Extreme Weather
[5] *Cyber-Informed Transmission Planning Roadmap for Integrating Cyber Security into Transmission Planning*, May 2023 is being applied to this initiative under Energy Scenarios: ERO Enterprise Whitepaper on Cyber Planning 2023

related scenario sections. When the benchmark event results in cascading outages, uncontrolled separation, or instability, performance is not achieved and planners must develop a corrective action plan.[6]

This document constitutes the technical justification and technical foundation[7] for the development of energy scenarios.

Related Activities

Before moving forward, it is important to clarify how the energy scenario justification and associated SAR effort differs from other NERC standards development projects and subcommittee activities involving the suite of Transmission Planning (TPL) Reliability Standards in **Table 1**.

Table 1: Related TPL Activities

Effort	Focus	Study Interval
Energy Scenarios (this effort)	Analyses focused on identifying transmission system performance in the long-term planning horizon using power flow models (excluding the Order No. 896 directive)	Specific points in time in the 6–10-year period
Project 2020-02 Modifications to TPL-001 and MOD-032	Consideration of DER in TPL-001-5.1	Annually
Project 2023-07 Extreme Heat and Cold Weather (i.e., Order No. 896)[8]	Analyses focused on identifying transmission system performance in the long-term planning horizon using power flow models	Specific points in time in the 6–10-year period
Energy Reliability Assessment Task Force (ERATF)[9]	Assessments focused on supplying energy in the Operations time horizon using tools and generally other than power flow models	Usually, every hour over the span of a year
Energy Reliability Assessment Task Force	Assessments focused on supply energy in the near-term and long-term planning time horizon using probabilistic methods and generally other than power flow models	The 1–5 year, Mid-Term, and 5–10-year periods
System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG)[10]	The SPIDERWG focus is modeling data and parameters of DER for transmission planning models	Near-term and long-term planning horizon
Security Integration and Technology Enablement	Analysis of cyber security risks in transmission planning	Long-term planning horizon

[6] The corrective action plan used herein implies the same use as defined by the *Glossary of Terms* used in NERC Reliability Standards, which is "A list of actions and an associated timetable for implementation to remedy a specific problem." A plan can propose infrastructure investment or modifications as well as other alternatives such as operational procedures.
[7] See: https://tyndp.entsoe.eu/explore/discover-the#
[8] Project 2023-07–Modifications to TPL-001-5.1 *Transmission System Planning Performance Requirements for Extreme Weather*: Project 2023 07 Mod to TPL00151
[9] Project 2022-03 Energy Assurance with Energy-Constrained Resources
[10] See: SPIDERWG

Table 1: Related TPL Activities		
Effort	**Focus**	**Study Interval**
Subcommittee (SITES)[11] and Security Working Group (SWG)[12]		
Project 2022-04 Electro-Magnetic Transient (EMT) Modeling[13]	The EMT drafting team is focused on addressing the accuracy of model data needed for EMT studies, when to conduct studies, and what facilities must be studied.	Interconnection process and long-term planning

Transmission Planning Energy Scenarios

Transmission planning energy scenarios refer to the process of ensuring adequate BPS performance for a given electrical and/or geographic area and analyzing potential future supply and demand scenarios. These are typically used to inform the buildout of transmission infrastructure. These scenarios may include projections for electricity generation from different sources (e.g., coal, natural gas, solar, wind), estimates of energy demand from various sectors (e.g., residential, commercial, industrial), and assessments of potential changes in energy policies, regulations, and technology advancements in how energy is generated or consumed. Some of these projections come from state-sponsored programs, others from utility initiatives, and even some from policy statements and stakeholder input.

The purpose of these scenarios is to ensure BPS performance[14] in order to understand how the energy needs of an area can be met reliably. Transmission planning energy scenarios are an important part of the overall planning process, inform the feasibility of policy decisions, and potentially drive investment in new infrastructure.

Energy Scenarios

Energy scenarios evaluate transmission system performance under the various situations defined in the benchmark events that are not studied in traditional planning cases. Steady-state events are performed analogous to the TPL-001-5.1 Category P0 condition (i.e., no contingency), and stability analyses mimic contingency Categories P1–P7 depending on the scenario studied. Incorporating defined energy scenarios into transmission planning benchmark events (specific cases) will reveal areas of the BPS that need to be mitigated when the benchmark event results in cascading outages, uncontrolled separation, or instability. The following energy scenarios are considered a minimum when applied to the aforementioned areas of concern regarding extreme natural events, natural gas/electricity interdependencies, and distributed energy resource impacts:

- **De-carbonization and Policy Scenario:** This scenario assumes variations in the resource mix based on drivers like regulatory policy or economic forces. TPs use this scenario to identify BPS performance issues related to the shifts in the resource characteristics.

[11] See: RSTC SITES
[12] See RSTC SWG
[13] See Project 2022-04 EMT Modeling (nerc.com)
[14] Including lines, substations, and Protection System enhancements.

- **High Renewables Penetration Scenario:** This scenario assumes a significant shift towards low-carbon energy sources, such as wind, solar, and hydro. TPs can use this scenario to identify the transmission infrastructure required to connect new renewable energy sources to the BPS and ensure that the BPS is expected to meet performance standards given the intermittent nature of renewable energy generation. Considering a high renewable penetration resource mix identifies resources that could be more susceptible to long-term, widespread extreme natural events. Such events should include extreme high and low temperature conditions, lack of irradiance (solar) and lack of wind (wind), and any water (drought or surplus) conditions impacting hydro-electric resources can reveal potential energy constraints.
- **High Demand Scenario**: This scenario assumes a significant increase in energy demand due to increasing electrification. TPs use this scenario to identify issues where the gross load is masked by renewable resources. For example, high demand can occur when behind-the-meter solar output is reduced resulting in increased load that is coincident with BPS-connected solar resources that are simultaneously experiencing lowered generation output.
- **Technology-Driven Scenario:** This scenario assumes significant advancements in energy storage, demand response, or other energy management technologies that have not reach maturity. TPs can use this scenario to identify areas where a specific technology is being integrated into the BPS infrastructure and address any reliability concerns on the expected performance of the BPS.
- **Control and Communication Scenario:** This scenario assumes potential interruption in the ability to control portions of the BPS that could be due to an equipment or communication backbone issue. A loss of control or communications can affect numerous resources within a local area or dispersed resources across a wide area. Understanding how resources are controlled and the associated communication paths will enable planners to study these impacts affecting multiple resources.
- **Loss of Output Scenario:** This scenario assumes that the output of certain resources can become disrupted due to widespread fuel constraints. A couple examples include long-term natural gas pipeline, supply, or processing disruptions or weather pattern changes (e.g., low solar irradiance, low wind, drought). TPs can use this scenario to study the effects of output across varying resource types separately and together.

Ultimately, TPs should consider a range of energy scenarios to ensure that the BPS infrastructure is resilient, reliable, and flexible enough to meet the energy demands of the future. By developing and optimizing the BPS infrastructure, TPs can help ensure that energy is delivered safely, efficiently, and reliably to end-use customers.

In addition to the energy scenarios described above, TPs must also consider both normal and extreme natural events when developing their transmission plans. Normal events are those that are expected to occur with some regularity and can include changes in energy demand due to seasonal fluctuations, planned resource retirements, and the addition of new energy resources to the BPS. Extreme events, on the other hand, are those that are less predictable and can include severe weather events, and natural disasters.

NERC TPL-001 Reliability Standard Review

Reliability Standard TPL-001-5.1[15] establishes transmission system planning performance requirements that ensure the BPS will perform reliably over a broad spectrum of system conditions and following a wide range of probable contingencies. The Reliability Standard sets out requirements for modeling and conducting annual transmission planning assessments for both steady-state and stability system behavior. Contingencies must be applied to the planning models by the TP to identify areas where corrective action is required to meet performance requirements. Assessments must include the electric system composition for the near-term (0-5 years) and for long-term (6–10 years) planning horizons and beyond.

The following observations were noted[16] concerning the currently effective TPL-001 Reliability Standard:

- The Reliability Standard does not explicitly define or require the study of energy scenarios.
- There are no clear requirement(s) for the study of extreme natural weather or other environmental events.
- There is no consideration of a wide-area natural gas supply disruption or being curtailed during high demand.
- It does not require the assessment of DER impacts on the BPS.

Furthermore, there is no existing study requirements of common mode failure[17] in TPL-001 beyond the set of the identified criteria in Table 1 of the Reliability Standard. Understanding simultaneous failures and interdependencies, especially for critical infrastructure, is critical to identifying potential impacts on BPS.

Transmission Planning Standard (TPL-001) Enhancement Needs

Increased changes in the energy landscape with extreme weather events, natural gas/electricity interdependencies, the growth of renewable resources, and the increase in DERs[18] have raised new challenges for transmission planning. NERC Project 2022-02 aims to revise TPL-001 to provide clarity and consistency for how BPS-connected inverter-based resources are considered, modeled, and studied in planning assessments.

The proposed revisions to TPL-001 will ensure industry is effectively, efficiently, and consistently conducting planning assessments and that the requirements are equally suitable for inverter-based resources as they are for synchronous generation. The requirements should be revised to provide clarity or, in some cases, expand the scope of requirements when considering the performance of DERs to ensure the accuracy of transmission system planning assessments address energy-related scenarios.

These changes necessitate modifications to TPL-001 to ensure that it remains effective in identifying potential BPS performance risks associated with these challenges. Failure to address these issues could

[15] TPL-001-5.1 – Transmission System Planning Performance Requirements .
[16] Energy Assessment Technical Justification, updated May 5, 2022.
[17] Common mode failure refers to the simultaneous or near-simultaneous failure of resources due to a single event.
[18] Currently, Project 2022-02 is established to revise TPL-001-5.1 to include clarity for DERs.

result in a range of negative consequences, including widespread instability, uncontrolled separation, and cascading. In addition, failure to address these issues could lead to increased costs for electricity customers as transmission owners and operators are forced to implement reactive mitigating measures to address reliability issues.

Approaches to transmission planning have been based primarily around traditional methods with only a few areas considering progressive approaches to non-traditional planning issues. Historical data is the primary driver for determining forward-looking projections of growth and demand but not for the effects of resource variability, changes in technology, electrification, and consumer behavior. Energy scenarios expand transmission planning in order to reveal performance issues based on specific defined events that are possible.

Traditional transmission planning processes have evolved around performing sensitivity analysis that involves testing how the power system would behave under different conditions or assumptions. These tests are usually based on a varied set of predetermined parameters to see how the system would react. For example, a sensitivity analysis might vary assumptions about future demand growth, the planned resource dispatch due to fuel prices, or the availability of generating resources to understand how the system would behave under different scenarios. TPL-001-5.1 requires that one or more of the specified sensitivities (e.g., real and reactive load, expected transfers, controllable loads and demand side management) be varied in the near-term planning horizon but does not require them to be simultaneously varied. Sensitivities for energy scenarios must study simultaneous variations in defined sensitivities (e.g., related load, generation, and transfers). Also, these assumptions are not required to be coordinated with other TPs to ensure validity across a wide area.

The proposed energy scenarios, on the other hand, are a set of defined possible futures that are used to assess the ongoing needs of the BPS similar to the analysis forecasters use to project the future demand, generation, or adoption of a specific technology. Energy scenarios typically consider a range of factors that may impact the demand for electricity and the mix of generating resources, such as changes in technology, policy, and consumer behavior.

Adding energy scenarios to the present transmission planning and sensitivity analyses will greatly enhance the efficiency, effectiveness, and consistency of the planning process in identifying potential BPS performance risks associated with these present and continuing challenges. Sensitivity analyses will help identify potential problems and determine the most effective solutions to address them. Energy scenarios, on the other hand, provide a framework for understanding how the electricity system may evolve over time and help ensure that the transmission system is built to meet the needs of customers today and in the future. In summary, energy scenarios and sensitivity analyses are complementary tools that are both essential for ensuring a reliable and resilient BPS.

The ERO Enterprise team recommends having multiple planning NERC Reliability Standards for each energy scenario category under a suite of transmission planning standards that cover the commonality among all of them while modifying and updating TPL-001 to ensure consistency. One reason is that TPL-001-5.1 requires annual assessments, and these are anticipated to have a periodicity of 3–5 years that will be

determined through the standards development process. **Figure 1** shows a depiction of what could be implemented.

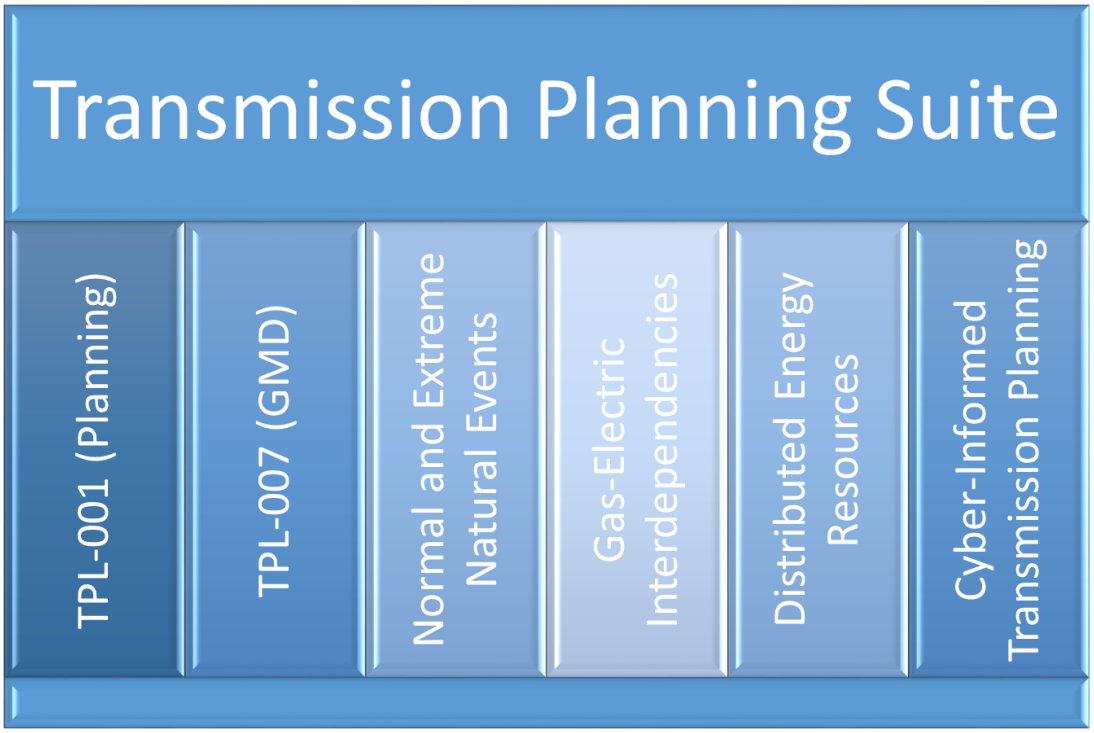


Figure 1: Suggested Suite of Transmission Planning Standards (Existing TPL-001 and TPL-007, and Potentially Four Energy Scenario Standards)

Normal and Extreme Natural Events

The challenges in transmission planning due to extreme patterns have been highlighted by recent extreme weather-related occurrences that affected vast areas of the continent over the past ten years. Hence, BPS reliability has been significantly impacted by the recent extreme heat and cold occurrences. However, as part of transmission system planning, the possible effects of widespread extreme natural events on BPS reliability can be estimated and examined in advance by using benchmark events. The findings will be used by TPs to create strategies that could be implemented by the applicable entity in advance of and in preparation for both normal and extreme natural events over a wide area through corrective action plans. Such corrective action plans and mitigation, for instance, might require more contingency reserves by the applicable entity or implement new energy-saving initiatives to reduce load, or call for more interregional transfer capability, switch or reconfigure transmission lines, or modify transmission and generation maintenance outages based on longer-lead times forecast as well as additional system upgrades and reinforcements.

Normal and Extreme Natural Event Benchmark Events

Benchmark events are necessary to establish a baseline for energy scenario studies. These events must be developed in collaboration and coordination with other TPs whose systems may be impacted or called upon to provide energy-related support. The following benchmark normal and extreme natural events should be

based on their respective categories and consider the approaches provided in this paper and/or use the expertise of the subject matter experts tasked with developing a new or modified Reliability Standard. Normal natural events that TPs should consider include the following:

- **Seasonal Demand Variations:** TPs can analyze historical energy consumption patterns to identify times of the year when energy demand is highest or lowest. They can then plan for re-powering or outages based on maintenance intervals during times of lower demand to minimize risks to the BPS when all elements are not in service.
- **Planned Energy Resource Additions:** When new energy resources are added to the BPS, such as wind or solar power plants, TPs must ensure those resources are incorporated into the planning analyses process.
- **Resource Variability:** Cases should be based on major prior normal meteorological projections as well as resource variations caused by intrinsic solar and wind variability.

Extreme natural events that TPs may consider include the following:

- **Severe Weather Events:** Extreme weather events, such as hurricanes, tornadoes, heat waves, fires, and winter storms, can limit or damage transmission infrastructure, potentially leading to widespread instability, uncontrolled separation, and cascading. TPs must prepare for these events by identifying vulnerable facilities in advance and determining whether these facilities should be considered unavailable during severe weather events. Identified vulnerabilities can be mitigated in advance by investing in improvements or redundancy to reduce the risks from severe weather events.
- **Natural Disasters:** Natural disasters, such as earthquakes or wildfires,[19] can limit or damage transmission infrastructure (or other infrastructure such as a natural gas pipeline) and disrupt the normal flow of energy, potentially leading to weakened transmission operating conditions and capability. TPs must proactively plan for these events by identifying critical infrastructure and developing contingency plans for repair and restoration.
- **Resource Variability:** Cases should be based on major prior extreme weather events. Variations in resources caused by heat and cold temperature extremes (Order No. 896), solar and wind variability, drought and flooding propensity, atmosphere contamination (e.g., volcanic ash, fog, smog, smoke) and its propagation, storm-prone (e.g., derechos, hurricanes, polar vortexes) areas, and consider the study of other potential natural disasters and events.

There are factors that affect the scope of transmission planning energy scenarios and benchmark events. Factors that must be considered to ensure that scenarios and associated normal and extreme natural events remain consistent, reasonable, and representative of the planning area include the following:

- Identifying geographical regional differences in climate and weather patterns
- Using extreme natural event meteorological data from reliable sources (e.g., national laboratories; regional transmission operators; the National Oceanic and Atmospheric Administration; Environment Canada; and other local, state, and federal agencies and organizations)

[19] Wildfire Mitigation Reference Guide, January 2021

- Applying a common method to follow when creating benchmark events
- Potential event-related coincident contingencies (e.g., concurrent/correlated generation and transmission outages, derates) and expected future conditions of the system, such as changes in load
- Available transfers
- Generation resource mix
- Identifying facilities sensitive to certain events

Conduct Studies for Normal and Extreme Natural Benchmark Events

The need is not to apply all the contingencies (e.g., Categories P1-P7) set forth in TPL-001. Planners will model their respective areas using benchmark events and energy scenarios spanning the long-term planning horizon. Steady-state and stability analysis cases will be conducted for the various energy scenarios using defined sensitivity testing (coordinated among TPs) to test the assumptions of the benchmark events. In cases where BPS performance cannot be met, planners must develop and implement corrective action plans to mitigate the risk.

Steady State and Transient Stability Analyses

In a steady state analysis, the system components are modeled as either in-service or out-of-service, and the result is a single point-in-time snapshot of the system in a state of equilibrium. A transient stability (dynamic) analysis examines the system from the start to the end of a perturbation to determine if the system returns to a state of equilibrium. Performing both analyses ensures that the system has been thoroughly assessed for instability, uncontrolled separation, and cascading failures in the steady-state and the transient stability realms. Methods and assumptions must be collaborated, coordinated, and communicated among neighboring TPs to ensure consistency across a wide area.

Steady-State

The steady-state analyses need to assess system performance under no contingencies (e.g., Category P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Conducting the following steady-state studies can reveal performance issues in the normal system configuration for specific energy scenarios and extreme natural events over the long-term planning horizon.

Steady-state studies must accomplish the following:

- Apply normal and extreme natural weather benchmark events
- Apply the benchmark events to each defined energy scenarios
- Include specific defined criteria for determining which concurrent and correlated outages of both generators and transmission lines
- Model demand load response in benchmark event cases as a corrective action to meet system performance criteria
- Evaluate the wide-area performance during such benchmark events for the defined energy scenarios

Stability

The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies but not necessarily while mirroring TPL-001 planning contingencies (e.g., Categories P1-P7). Since the goal of energy scenario transmission planning is based on energy-related variability, dynamic studies need to consider the rapid change in dispatch over a wide area. Examples include the common mode loss of inverter-based resources, unforeseen changes in wind according to forecasts impacting wind generation, and unanticipated cloud coverage impacting solar resources. Conducting the following stability studies can reveal performance issues for specific energy scenarios for normal and extreme natural benchmark events over the long-term planning horizon.

Stability studies must perform the following:

- Apply normal and extreme natural weather benchmark events
- Apply the defined energy scenario contingencies (e.g., high demand and low resource availability) to each benchmark event
- Include specific defined criteria for determining which concurrent and correlated unplanned outages of both generators and transmission lines
- Model demand load response in benchmark event cases as a corrective action to meet system performance criteria
- Evaluate the wide-area performance during such benchmark events and energy scenarios

Sensitivity Analysis

Sensitivity analyses help a TP to determine if the performance results of the base case are sensitive to variations of the energy scenario inputs. The use of sensitivity analyses is particularly necessary when studying normal and extreme natural events because some of the assumptions made when developing a traditional transmission planning base case may change depending on the extreme weather condition as required by TPL-001-5.1.[20] For example, during extreme natural events, load may increase as temperatures decrease (i.e., winter storm) all while a decrease in temperature may result in a decrease in generation output or availability. The sensitivity analysis must go beyond the typical TPL-001 studying sensitivities (e.g., load, generation, transfers) independently and consider more than one sensitivity occurring simultaneously.

Sensitivity assumptions must be documented and must be applied to the benchmark events and energy scenarios. The following are minimum considerations in conducting sensitivity analyses:

- Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark event
- Establish a baseline set of sensitivities that include conditions that vary with temperature such as load, generation, and system transfers

[20] See TPL-001-5.1, Table 1 – Steady State & Stability Performance Extreme Events, Steady State, note 3a(iv).

Natural Gas/Electricity Interdependencies

The challenges in transmission planning due to natural gas/electricity interdependencies have been highlighted by recent events[21] that affected vast areas of the nation over the past ten years. Hence, BPS reliability has been significantly impacted by natural gas disruptions. However, as part of transmission system planning, the possible effects of widespread reliance on natural gas on BPS reliability can be estimated and examined in advance by using benchmark events. The findings can be used by TPs to create strategies for corrective action plans with mitigation that could be implemented by the applicable entity in advance of and in preparation for potential pipeline disruptions or unanticipated natural gas curtailments over a wide area. Such corrective action plans, for instance, might plan for more contingency reserves by the applicable entity or implement new energy-saving initiatives to reduce load or require dual-fuel resources. They might also plan for more interregional transfer capability, switch or reconfigure transmission lines.

The electric grid and the natural gas network are two of the most critical infrastructure systems in North America. They are also closely interconnected, and their reliability depends on each other. The proliferation in the last two decades of new natural-gas-fired generators served from common supply pipelines, may experience a natural gas system disturbance whose impact is more severe than the loss of a single generator, transmission line, or transformer. A single natural gas contingency, such as the interruption or pressure loss of a single natural gas pipeline, may result in the loss of multiple electric generators. With proper planning and unit design, the impacts of natural gas pipeline contingencies can be mitigated. Hence, natural gas/electricity interdependencies must be considered in transmission planning because they can have a significant impact on BPS reliability.

Natural Gas Interdependency Benchmark Events

Natural gas/electricity interdependency refers to the complexities between natural gas and electric power systems. Natural gas has grown as an important and primary fuel source for a substantial portion of generation, and in many cases electric power is often required to power natural gas production, gathering, processing, and delivery infrastructure, such as the electrically-driven pumps and compressors that transport the natural gas through pipelines to the BPS generation facilities. Also, the dependence on natural-gas-fired generation to assure BPS reliability does not always align with the regulatory construct and weatherization requirements for natural gas production, gathering, and delivery systems. This is particularly evident during severe cold weather when high demand for natural-gas-fired generation occurs coincident with natural gas service essential for end use consumers. Therefore, TPs must consider the interdependencies between these two demands on the natural gas systems when developing their benchmark transmission events.

Transmission planning benchmark events are necessary to establish a baseline for energy scenario studies. These events must be developed in collaboration and coordination with other BPS TPs whose systems may be impacted or called upon to provide energy support. The following benchmark events should be based on their respective natural gas/electricity interdependencies considering the approaches provided in this paper or using the expertise of the subject matter experts tasked with developing a new or modified

[21] For example: Special Reliability Assessment: Potential BPS Impacts Due to Severe Disruptions on the Natural Gas System

Reliability Standard. Benchmark event cases need to be based on the potential for future major pipeline disruptions, curtailments, or industry studies.

Benchmark events that TPs should consider with respect to natural gas/electricity interdependencies include the following:

- **Natural Gas Supply Disruptions:** Natural gas supply disruptions can occur due to pipeline maintenance, severe weather events, or geopolitical tensions. These disruptions can impact generation by reducing the availability of natural-gas-fired power plants. TPs can prepare for these events by identifying the natural gas production, gathering, processing and pipeline infrastructure that is critical to maintaining generation availability, perform studies, and developing contingency plans for alternative fuel sources or demand response measures.
- **Electric Power Supply Disruptions:** Electric power supply disruptions to the natural gas pumps and compressors can impact the operation of natural gas production, gathering and pipelines by causing a reduction in flow and a drop in pipeline pressure below the level needed to supply BPS generators. TPs can plan for these events by identifying critical BPS infrastructure that supports natural gas production, gathering, and pipeline operation; then develop contingency plans for alternative sources of electric supply or implement energy storage systems. The natural gas pipeline infrastructure exists beyond a local area; therefore, TPs need to understand and model the natural gas infrastructure employing a wide-area view (i.e., effects from events outside of a specific area that can have impact on that area), so the impacts can be understood and mitigated.
- **Fuel Switching:** Changes in the relative prices of natural gas and other fuels, such as coal or renewable energy sources, can impact the utilization of natural-gas-fired power plants. TPs can plan for these events by identifying the potential impacts of fuel switching on natural gas pipeline operations and developing plans for adjusting pipeline operations to accommodate changes in power generation.
- **Renewable Energy Integration:** As renewable energy sources, such as wind and solar become a larger share of the electric power resource mix, natural-gas-fired power plants are generally relied upon to provide balancing, regulation, and replacement energy as a backstop to variability of renewable resources. TPs can plan for these grid resource transformation type events by identifying the natural gas infrastructure that is critical to offsetting the variability of renewable resources and develop contingency plans for addressing constraints that might occur in the natural gas system that may render natural-gas-fired resources unavailable for providing essential reliability services and replacement energy.

Conduct Studies for Natural Gas/Electricity Interdependency Benchmark Events

The need is not to apply all the contingencies (e.g., Categories P1-P7) set forth in TPL-001. Planners will model their respective areas using benchmark events and energy scenarios spanning the long-term planning horizon. Steady-state and stability analysis cases will be conducted for the various energy scenarios using defined sensitivity testing (coordinated among TPs) to test the assumptions of the benchmark events. In cases where BPS performance cannot be met, planners must develop and implement corrective action plans to mitigate the risk.

Steady State and Transient Stability Analyses

In a steady state analysis, the system components are modeled as either in-service or out-of-service and the result is a single point-in-time snapshot of the system in a state of equilibrium. A transient stability (dynamic) analysis examines the system from the start to the end of a perturbation to determine if the system returns to a state of equilibrium. Performing both analyses ensures that the system has been thoroughly assessed for instability, uncontrolled separation, and cascading failures in both the steady-state and the transient stability realms. Methods and assumptions must be collaborated, coordinated, and communicated among neighboring TPs to ensure consistency across a wide area.

Steady-State

The steady-state analyses need to assess system performance under no contingencies (e.g., Category P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Conducting the following steady-state studies can reveal performance issues in the normal system configuration for specific energy scenarios and natural gas/electricity interdependency events over the long-term planning horizon.

Steady-state studies must perform the following:

- Apply natural gas/electricity interdependency benchmark events
- Apply the defined energy scenarios to each benchmark event
- Include specific criteria for determining which concurrent and correlated outages of both generators and transmission lines
- Model demand load response in benchmark event cases as a corrective action to meet system performance criteria
- Evaluate the wide-area performance during such benchmark events and energy scenarios

Stability

The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies but not necessarily while mirroring TPL-001 planning contingencies (e.g., Categories P1-P7). Since the goal of energy scenario transmission planning is based on energy variability, dynamic studies need to consider the rapid change in dispatch over a wide area. Examples include the common mode loss of inverter-based resources, unforeseen change in wind according to forecasts impacting wind generation, and unanticipated cloud coverage impacting solar resources. Conducting the following stability studies can reveal performance issues for specific energy scenarios and natural gas/electricity interdependency benchmark events over the long-term planning horizon.
Stability studies must perform the following:

- Apply natural gas/electricity interdependency benchmark events
- Apply the defined energy scenario contingencies (e.g., high demand, low resource availability, fuel switching) to each benchmark event
- Include specific criteria for determining which concurrent and correlated unplanned outages of both generators and transmission lines

- Model demand load response in benchmark event cases as a corrective action to meet system performance criteria
- Evaluate the wide-area performance during such benchmark events and energy scenarios
- Evaluate risks of compressor stations electric motors stalling

Sensitivity Analysis

Sensitivity analyses help a TP to determine if the performance results of the base case are sensitive to variations in the energy scenario inputs. The use of sensitivity analyses is particularly necessary when studying natural gas/electricity interdependency events because some of the assumptions made when developing a traditional transmission planning base case may change if there is more than one loss of a large natural gas pipeline into an area or multiple areas that have significant natural-gas-fired generation as required by TPL-001-5.1.[22] For example, during natural gas/electricity interdependency events, load may increase as temperatures decrease (i.e., winter storm) all while a decrease in temperature may result in a decrease in available fuel for generation output or availability. The sensitivity analysis must go beyond the typical TPL-001 study sensitivities (e.g., load, generation, and transfers) independently and consider more than one sensitivity occurring simultaneously.

Sensitivity assumptions must be documented and must be applied to the benchmark events and energy scenarios. The following are minimum considerations in conducting sensitivity analyses:

- Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark event
- Establish a baseline set of sensitivities that includes conditions that vary with temperature, such as load, generation, and system transfers

Distributed Energy Resources

Currently, TPL-001-5.1 is under revision for inclusion of DERs stemming from the System Planning Impacts of Distributed Energy Resources Working Group assessment on TPL-001.[23] The working group stepped through the requirements to determine if they were relevant to DERs in the assessment. The group also discussed how DERs can be included in that portion of the annual planning assessment performed under TPL-001-5.1. The group identified that DERs (a source of electric power on the distribution system) should be included as part of the TPL-001 contingencies; however, the assessment did not address or provide guidance on energy scenarios due to those being a new concept in transmission planning. Instead, this *Transmission Planning Energy Scenarios* document addresses this issue.

DERs displace bulk-system generation as they lower the demand required to be served by the transmission system. Hence, attention to their capacity and deliverability to load is an important consideration in energy assessments. This is doubly important in areas where back feeding on the transmission system occurs. Currently, DERs are a source of “must-take” power generation, so they may be masking current gross load quantities at the transmission to distribution interface that a utility must serve should DERs become

[22] See TPL-001-5.1, Table 1 - Steady State & Stability Performance Extreme Events, Steady State, note 3a(i).
[23] Available here: SPIDERWG White Paper TPL-001 Assessment

unavailable due to equipment failure, lack of sufficient fuel,[24] or other outage condition. Thus, the inclusion and treatment of DERs in transmission planning benchmark events and energy scenarios should be planned for to ensure that the interconnected BPS is planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Reliability Standards.

DER Benchmark Events

DERs are any source of electric power on the distribution system. These include resources that inject power into (e.g., synchronous DERs and asynchronous solar ("photovoltaic" DERs)) and exchange power (e.g., chemical battery storage DERs) with the distribution system. These resources are located close to the point of consumption and can provide a range of benefits for the BPS, including improved reliability, reduced resistive electrical losses, and lower overall costs. However, the integration of DERs into the distribution system and interconnection to the BPS at the T-D interface can also create challenges for TPs, who must ensure that the BPS infrastructure can handle the autonomy, variability, and intermittency of these resources.

Benchmark events that TPs may consider with respect to DERs located in the distribution system include:

- **High DER Penetration:** As more consumers adopt DERs, the total amount of power that is generated and consumed locally may vary significantly, challenging historic assumptions on the "peak" and "off-peak" power points. TPs can plan for this high penetration by calculating the anticipated maximum DER penetration level based on data provided by the distribution entity and projecting the potential penetration due to actual trends or policy changes. Planners can also consider the potential benefits of storage-based DERs during peak periods. For example, storage-based DER as a generation asset and not demand response.
- **DER Variability:** DERs in the aggregate can vary widely, creating challenges for BPS operators who must balance the supply and demand of electric power in real-time. TPs can plan for these scenarios by evaluating the potential impact of the extreme limits of variability and resulting net load swings on BPS performance and developing contingency plans and corrective action plans for managing this variability.
- **DERs Effects on BPS:** DERs can provide a range of support services for the BPS, such as frequency response support. TPs need to explicitly represent DER operating profiles in benchmark events. This can identify the potential benefits or detriment of DERs on BPS performance and lead to the development of plans for DERs located in the distribution system and interconnected to the BPS at the T-D interface. Enabling these DER features can mitigate impacts revealed in benchmark event studies.
- **DER Outage Scenarios**: DERs may experience outages due to weather events, equipment failures, common mode loss, or other factors. TPs can plan for these scenarios by identifying the common interdependencies where DERs are most likely to experience a lack of availability and developing contingency plans for maintaining BPS reliability during these outages.

[24] Note that DERs include synchronous and IBR facilities. Solar PV is only available during times of sufficient sunlight. Similarly, carbon fuel constraints for DERs can make synchronous DERs unavailable.

As many of the above bullets deal with the treatment of base case generation dispatch, treatment of capacity to response in simulation, and enhancements to already established credible contingencies, the inclusion of DERs in energy scenarios focuses primarily[25] on identifying the DER response to BPS conditions and capacity of DER in an area.

Conduct Studies for DER Benchmark Events

The need is not to apply all the contingencies (e.g., Categories P1-P7) set forth in TPL-001. Planners will model their respective areas using benchmark events and energy scenarios spanning the long-term planning horizon. Steady-state and stability analysis cases will be conducted for the various energy scenarios using defined sensitivity testing (coordinated among TPs) to test the assumptions of the benchmark events. In cases where BPS performance cannot be met, planners must develop and implement corrective action plans to mitigate the risk.

Steady State and Transient Stability Analyses

In a steady state analysis, system components are modeled as either in-service or out-of-service and the result is a single point-in-time snapshot of the system in a state of equilibrium. A transient stability (dynamic) analysis examines the system from the start to the end of a perturbation to determine if the system returns to a state of equilibrium. Performing both analyses ensures that the system has been thoroughly assessed for instability, uncontrolled separation, and cascading failures in the steady-state and the transient stability realms. Methods and assumptions must be collaborated, coordinated, and communicated among neighboring TPs to ensure consistency across a wide area.

Steady-State

The steady-state analyses need to assess system performance under no contingencies (e.g., Category P0 under TPL-001) with all system elements in-service with the anticipated generation dispatch. Conducting the following steady-state studies can reveal performance issues in the normal system configuration for specific energy scenarios and DER events over the long-term planning horizon.

Steady-state studies must perform the following:

- Apply the DER benchmark events
- Apply the defined energy scenarios (e.g., common mode loss, high demand, low DER availability) to each benchmark event
- Include specific criteria for determining which concurrent and correlated outages of both generators and transmission lines
- The analysis concerning the impacts of remand response must consider its affects the various studied energy scenarios in the benchmark events. Similarly, DER impacts must consider its effects on the various studied energy scenarios. DER in this context is generation assets and not load resources.
- Evaluate the wide-area performance during such benchmark events and energy scenarios

[25] As opposed to focusing on how each DER's protection may initiate a credible contingency. It is not prevalent that DERs cause frequency or voltage excursions at this time but rather exacerbate a BPS disturbance. This same treatment should be applied in transmission planning energy assessments.

Stability

The stability (i.e., dynamic) analyses need to assess the system performance under a defined contingency or set of contingencies but not necessarily while mirroring TPL-001 planning contingencies (e.g., Categories P1-P7). Since the goal of energy scenario transmission planning is based on energy variability, dynamic studies need to consider the rapid change in dispatch over a wide area. Examples include the common mode[26] loss of inverter-based resources, unforeseen changes in wind according to forecasts that impact wind generation, and unanticipated cloud coverage impacting solar resources. Conducting the following stability studies can reveal performance issues for specific energy scenarios and DER benchmark events over the long-term planning horizon.

Stability studies must perform the following:

- Apply the DER benchmark events
- Apply the defined energy scenario contingencies (e.g., common mode loss, high demand, low DER availability) to each benchmark event
- Include specific criteria for determining which concurrent and correlated unplanned outages of both generators and transmission lines
- The analysis concerning the impacts of demand response must consider its affects the various studied energy scenarios in the benchmark events. Similarly, DER impacts must consider its effects on the various studied energy scenarios. DER in this context is generation assets and not load resources.
- Evaluate the wide-area performance during such benchmark events and energy scenarios

Sensitivity Analysis

Sensitivity analyses help a TP to determine if the performance results of the base case are sensitive to variations in the energy scenario inputs. The use of sensitivity analyses is particularly necessary when studying DER events because some of the assumptions made when developing a traditional transmission planning base case may change if there is a common mode event (e.g., momentary cessation) TPL-001-5.1.[27] For example, during DER events, distribution load may increase suddenly due to cloud coverage when DERs (e.g., rooftop solar) reduce output and other renewable resources degrade output. During high temperatures, this may result in a decrease in generation output or availability. The sensitivity analysis must go beyond the typical TPL-001 study sensitivities (e.g., load, generation, and transfers) independently and consider more than one sensitivity occurring simultaneously.

Sensitivity assumptions must be documented and applied to the benchmark events and energy scenarios. The following are minimum considerations for conducting sensitivity analyses:

- Require the use of sensitivity cases to demonstrate the impact of changes to the assumptions used in the benchmark event

[26] Common mode interruption of DER have been documented abroad and in the US in at least two NERC reports, the April and May 2018 Fault-Induced Solar PV Resource Disturbances Report (January 2019), and San Fernando Disturbance Report, (November 2020) leading to increased net load on the BPS.

[27] See TPL-001-5.1, Table 1 - Steady State & Stability Performance Extreme Events, Steady State, note 3b.

- Establish a baseline set of sensitivities that include conditions that vary with temperature such as load, generation, and system transfers

Additional Considerations

Approaches to Benchmark Events

It is clear from past experiences that traditional planning approaches are not revealing issues related to transmission planning energy scenarios and benchmark events. NERC is not recommending a specific approach but recognizes that the approach used in the TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events[28] Reliability Standard has merit. Therefore, subject matter experts should develop a new or modified Reliability Standard. These experts should consider alternative planning methods and techniques that diverge from past transmission planning methods to better capture the challenges posed by benchmark events. Experts must define one or more approaches to determining the bounds of benchmark events that must be studied and consider the following:

- Whether probabilistic techniques can be incorporated into the new or modified Reliability Standard and implemented by responsible entities, and
- If a probabilistic approach is feasible and reasonable, address factors like the following:
  - A projected frequency (e.g., 1-in-50-year event)
  - A probability distribution (95th percentile event)

Wide-Area Considerations

The North American BPS is comprised of numerous transmission planning entities. As such, transmission planning benchmark event studies must consider the wide-area impacts of benchmark events and energy scenarios. This paper does not aim to define the depth or breadth of the term “wide area" and defers to the continent-wide expertise of the subject matter experts tasked with developing a new or modified Reliability Standard.[29] These experts will be appointed through the *NERC Standard Processes Manual,*[30] which requires the involvement of experts from varying areas.

Concurrent/Correlated Generator and Transmission outages

Previous events have demonstrated, for example, that there is a high correlation between generator outages and cold temperatures, indicating that unplanned generator outages and derates increase as temperatures decrease. Because of this correlation, it is necessary for transmission planning studies to evaluate the risk of correlated or concurrent outages and derates of all types of generation resources and transmission facilities. Some generators may be unavailable under normal or extreme natural events, natural gas/electricity interdependency issues, or unanticipated DER loss, so potential outages must be considered in benchmark events and energy scenarios.

[28] NERC website at: https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-007-4.pdf.
[29] “Wide Area” is defined in the *Glossary of Terms* used in NERC Reliability Standards. The subject matter experts charged with defining “wide Area” will need to consider revising the defined term of creating a different term.
[30] See Appendix 3A of the NERC Rules of Procedure

Responsible Entities

The TPL-001-5.1 and TPL-007-4 Reliability Standards mandate that TPs are responsible for their specific planning areas and planning coordinators that oversee a number of transmission planning areas perform the Reliability Standard requirements. Since specific requirements and criteria to address benchmark events and energy scenarios have not been established, the paper defers to the expertise of the subject matter experts tasked with developing a new or modified Reliability Standard to determine the appropriate responsible entities. In doing so, beyond the expected inclusion of the TP and planning coordinator NERC functional entities, the experts must identify and include any other functional entities that have a responsibility for providing data and information, or any other identified BPS planning obligations during the course of developing a new or modified Reliability Standard. The experts must designate the functional entities responsible for developing wide-area studies in benchmark events. Additionally, the experts may use an existing functional entity or a group of functional entities (e.g., a group of planning coordinators) to designate the tasks of developing benchmark events, applying energy scenarios, and conducting wide-area studies.

Any effort considered in proposing to establish a new functional entity registration to undertake these tasks must be brought to the attention of NERC registration and legal staffs. The drafting, if considering such an approach, will need to consider that a new functional registration will require a modification to the NERC Rules of Procedure, which may be done in parallel with developing a new Reliability Standard or modifying TPL-001.

Coordination among Entities and Sharing of Data and Studies

In addition to determining the responsible entities that will be developing benchmark events, energy scenarios, and conducting wide area studies, there must be a mechanism in place to ensure the sharing of data and studies. For example, it is possible that the selected responsible entities under the new or modified Reliability Standard will not be able to request and receive needed data and information pursuant to MOD-032-1 – Data for Power System Modeling and Analysis.[31] Modification of MOD-032-1 may be required to ensure planners have the necessary data for modeling benchmark events and energy scenarios.

System information and study results sharing and coordination is necessary among TPs and planning coordinators with transmission operators, transmission owners, and generator owners for benchmark events and correction action plan implementation. Responsible entities must share the results of their wide area studies with other functional entities consistent with TPL-001-5.1 (e.g., transmission operators, transmission owners, and generator owners that have a reliability related need for the studies).[32]

Mechanism for Periodic Updates

Any transmission planning requires continual updating and analyses based on topology changes, resource mix changes, and demand profiles to name a few. Establishing a mechanism for the updating and conducting of studies needs to be consistent with the long-term planning horizon impacts (e.g., conducting a study every five years). Criteria developed to establish benchmark events and energy scenarios must have a defined periodicity for ensuring updates are timely and effective for transmission planning and meeting required BPS performance.

[31] See NERC Reliability Standards
[32] TPL-001-5.1 at Requirement R8

Corrective Action Plans

Corrective action plans are needed to ensure the interconnected BPS is planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Reliability Standards. Therefore, any instances where performance requirements for benchmark events and energy scenarios over a wide area are not met; corrective action plans must be developed that do the following:

- Identify-specified instances in benchmark events when performance standards are not met
- Establish required study contingencies and baseline sensitivities for which a corrective action plan is required
- Determine whether corrective action plans should be required for single or multiple sensitivity cases
- Determine whether corrective action plans should be developed if a benchmark event that is not already included in benchmark event would result in cascading outages, uncontrolled separation, or instability
- Require mitigation for specified instances where performance requirements for benchmark events and energy scenarios are not met (i.e., when certain benchmark studies conducted under the Reliability Standard show that a benchmark event would result in cascading outages, uncontrolled separation, or instability)
- Require that responsible entities share their corrective action plans with applicable regulatory authorities, including applicable governing bodies responsible for retail electric service issues

Conclusion

The issues raised in 2021 ERO Reliability Risk Priorities Report revealed that TPL-001 inadequately addresses energy scenarios specific to transmission planning for normal and extreme natural events, natural gas/electricity interdependencies, and the proliferation of DERs. As such, it reveals that TPL-001-5.1 must be modified, or a new Reliability Standard be developed to require TPs to study and understand the expected level of BPS performance over the range of the three areas when applying the various energy scenarios over a wide area. By applying energy scenarios, the TP can ensure that the transmission system is expected to perform at the required level of BPS performance in the following benchmark events:

- Extreme low or high temperatures, wind and solar variability, water availability (i.e., drought and flooding), fire, storms, and other natural disasters
- Pipelines with compressors, resources with no alternate energy option during a natural gas disruption, and natural gas curtailments due to heating demand
- DER output variability and predictability, back feeding the transmission system, and unknown actual demand on the transmission system

Requiring TPs to incorporate these areas within their planning assessments and studies will enhance the breadth of conditions the BPS could experience today and in the future. Applying appropriate energy scenarios and sensitivity analyses will reduce the likelihood of widespread instability, uncontrolled separation, and cascading.

Appendix B: Contributors

An ERO Enterprise team consisting of NERC and NERC Regional Entity staff was formed to develop this paper:

Name	Entity
John Idzior	ReliabilityFirst
Neeraj Lal	NPCC
Gaurav Karandikar	SERC
Brad Woods	Texas RE
Dianlong Wang	MRO
Enoch Davies	WECC
Scott Barfield-McGinnis	NERC
Mohamed Osman	NERC
William Lamanna	NERC

Risk Management for Third-Party Cloud Services

Action

- Accept the Risk Management for Third-Party Cloud Services Standard Authorization Request (SAR);
- Authorize posting of the SAR for a 30-day formal comment period; and
- Authorize solicitation of the drafting team (DT) members.

Background

From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks, and security teams are seeking tools and capabilities to improve their security programs. Security solutions with greater visibility, detection, correlation, analytics, and responsiveness are available using cloud services to help security teams reduce potential impacts of security events and speed recovery while protecting data confidentiality and integrity. Cloud services can provide increased availability, including resiliency, due to scalability, redundancy, high availability, and fault tolerance. Cloud services are critical in delivering excellent capability across security domains. Additionally, as noted in the 2020 FERC Notice of Inquiry[1], many new products from vendors are cloud-based solutions, placing increased pressure on NERC-registered entities to operate the Bulk Electric System (BES) securely.

Cloud services are needed due to the increasing data volumes required and the increasing need for data analytics and resources such as computing, network, and storage. Rapid deployment and integration of net zero energy systems (e.g., renewables) will rely on advanced monitoring, control, and data methodologies, such as machine learning (ML), that require scalable computing power. Phasor Measurement Units (PMUs) are among the monitoring devices that drive the need for cloud-based processing and storage.

Summary

Risk Management for Third-Party Cloud Services SAR aims to establish risk-based, outcome-driven requirements that align cloud services with other third-party resources already used for CIP-regulated systems, including BES operations and supporting cyber assets. This project will allow, but not require, cloud services for CIP-regulated systems, including BES operations and supporting cyber assets. NERC staff recommends that the Standards Committee accept the SAR, authorize posting for a 30-day formal comment period, and authorize the solicitation of drafting team members.

[1] Docket No. RM20-8-000 Virtualization and Cloud Computing Services, February 20, 2020, paragraphs 12 and 19.

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:	Cyber Security - Risk Management for Third-Party Cloud Services		
Date Submitted:	July 25, 2023		
SAR Requester			
Name:	• Rudolf Pawul, Vice President Information & Cyber Security Services • Joseph Mosher, NERC Portfolio Manager		
Organization:	• ISO New England and the ISO-RTO Council IT Committee • EDF Renewables		
Telephone:	R. Pawul: 413-540-4249 J. Mosher: 470.985.4050	Email:	rpawul@iso-ne.com joseph.mosher@edf-re.com

SAR Type (Check as many as apply)	
☒ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☒ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☒ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks and security teams are seeking tools and capabilities to improve their security programs. Security solutions with greater visibility, detection, correlation, analytics, and responsiveness are available using cloud services to help security teams to reduce potential impacts of security events and speed recovery while also protecting data confidentiality and integrity. Cloud services can provide increased availability including resiliency due to the scalability, redundancy, high availability, and fault tolerance. Cloud services play a critical role in providing greater capability across the security domains. Additionally, as noted in the 2020 FERC Notice of Inquiry[1], the vast majority of

[1] Docket No. RM20-8-000 Virtualization and Cloud Computing Services, February 20, 2020, paragraphs 12 and 19.

Requested information

new products from vendors are cloud-based solutions placing increased pressure on NERC registered entities to securely operate the BES.

Concurrently, from an operational and reliability perspective, the modern power grid landscape is changing, driven by rapid grid modernization, digital transformation, decentralization of electric resources and decarbonization targets. These factors are increasing the data volumes required to continue operating a reliable and resilient grid and thus increasing the need for data analytics and resources such as computing, network, and storage.

The U.S. Energy Information Administration projects that renewable generation will supply 44% of U.S. electricity by 2050[2]. To fully realize the national energy system decarbonization goals established by U.S. Federal and state Government Agencies, rapid deployment and integration of net zero energy systems will rely on advanced monitoring, control, and data methodologies, such as machine learning (ML) that require scalable computing power. Entity operations for assets across the NERC CIP impact levels will be facing the growing demands for compute capacity to manage the increasing volumes of data to respond to grid variability and maintain reliable grid operations. Agility and scalability will be a growing necessity to meet changing demands of grid operations, and cloud resources are essential in meeting such demands.

Renewable capacity expansion is accelerating. The International Energy Agency updated its growth projections in 2022, to an estimate of 359.5 GW in renewable capacity growth in the US, 2022-2027[3]. As renewable installations grow, site classifications may change from low to medium impact levels, putting operators at risk of having to revert to on-premises resources to meet compliance language rather than benefitting from the cloud services available to lower impact sites.

The advent of Phasor Measurement Units (PMUs), and the unprecedented need for rapid simulations to integrate renewables into a constrained network demand unprecedented amounts of data storage. Increasing data storage requirements and processing requirements of grid modernization are driving the need for cloud services. Cloud resources provide Entities with expanded simulation capabilities and development environments that can help meet patching cycles and testing requirements for on-premises assets under the CIP requirements.

Cloud computing is a priority for the US government as underscored by the CloudSmart strategy to accelerate government agency adoption of cloud-based solutions. Cloud has proven its value in other critical industries such as financial services, defense, and healthcare, and is a fitting option for grid applications. Cloud services offer fault-tolerant system design capabilities in which operations and data

[2] https://www.eia.gov/todayinenergy/detail.php?id=51698#:~:text=EIA%20projects%20that%20renewable%20generation,of%20U.S.%20electricity%20by%202050&text=Note%3A%20Biofuels%20are%20both%20shown,in%20petroleum%20and%20other%20liquids.

[3] https://www.iea.org/reports/renewables-2022/executive-summary

Requested information
can be replicated and run in independent application stacks in geographically dispersed locations along with other benefits, including reliability, resilience, and security. NERC standards revisions to CIP-004 and CIP-011 allow for the use of cloud storage for BES Cyber System information (BCSI). Comparable consideration is due other systems under the other regulated definitions or functions.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The project purpose is to establish risk-based, outcome-driven requirements that place cloud services on par with other third-party resources already used for CIP-regulated systems including for BES operations and supporting cyber assets. This project will allow, but not require, use of cloud services for CIP-regulated systems including BES operations and supporting cyber assets. This SAR proposes to create a new standard(s) or revise existing CIP Standards to address the language that includes or implies specific physical hardware and is preventing adoption of cloud services for regulated systems. As explained in NERC's 2019 whitepaper on "Virtualization and Future Technologies," the reliance on physical assets in the current standards prevents the use of cloud services in a compliant manner for some systems such as those defined as BES Cyber Systems or EACMS. The goals are to develop specific modifications to the CIP Standards, or create a new standard(s), to add clarity in allowing for the adoption and auditability of cloud services used for the BES. Creation of a new CIP Standard is strongly recommended. The goals also include addressing the role of third-party certifications as part of the auditability of the new or revised standards. These revisions will increase reliability and security to the Bulk Electric System (BES) by allowing the use of advanced technologies that support Entities in managing grid modernization and the changing grid landscape as well as making available to security teams all resources that can reduce potential impact and speed recovery from security events.
Project Scope (Define the parameters of the proposed project):
The project scope is to: • Create a new CIP standard(s) or revise the existing CIP standards to allow for adoption of cloud services for CIP-regulated systems. Creation of a new CIP standard is strongly recommended. • Require applicable entities that are procuring cloud services for CIP-regulated systems to develop and implement a plan to address the security objectives applicable to the use of cloud services for CIP-regulated systems including for BES operations and supporting cyber assets. • Determine a development plan to define whether revisions will be made to accommodate use of cloud for all CIP defined systems (such as EACMS, PACS, BCS, etc.) or if an incremental revisions

Requested information
approach will be taken to allow use of cloud for individual or groups of CIP-defined systems (such as first revising the standards to allow for EACMS use of cloud services). • Allow the use of third-party security certifications to support the auditability of the new or revised requirements. • Assess the applicability of the existing asset classifications (e.g., BES Cyber Assets (BCAs), BES Cyber Systems (BCS), and supporting cyber assets such as Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs), and Transient Cyber Assets (TCAs)) to determine which definitions apply with the new or revised standard(s), if any; determine if they require revision and, if so, revise accordingly; and, to determine if new definitions are needed and draft accordingly. Consider whether the function of systems within the definition classifications plays a relevant role in the standard(s) applicability (i.e. control functions versus non-control functions). • Coordinate with other CIP project drafting teams on conflicts or continuity matters, as necessary.
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] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
The following describes the proposed deliverables for this project: • New or revised standard(s) – the SDT will create risk-based and outcome-driven requirements within a new CIP standard(s) or in a revised CIP standard(s) to clarify the adoption of cloud services for CIP applicable systems and for regulated information[5]. It is strongly recommended that a new standard be created to allow entities to maintain their compliance programs for on-premises systems and assets under the existing CIP-002 thru CIP-014 suite of standards and to avoid conflicts that may occur in attempting to apply requirement language to physical and to cloud services. • The standard(s) will require applicable entities that are procuring cloud services for CIP-regulated systems to develop and implement a plan that addresses, at a minimum, the following specific objectives as they relate to cloud services for CIP applicable systems including for BES operations and supporting cyber assets: ○ Cloud service vendor risk management ○ Procurement controls The plan may apply different controls based on the criticality of different assets.

[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.

[5] Use of cloud for BES Cyber System Information is already covered by CIP-004 and CIP-011. Inclusion of BCSI in this revision project is at the discretion of the drafting team.

Requested information

Requirements developed by the SDT will be aimed at the protection of aspects of the cloud service that are within the control of the responsible entities.

- Holistic or incremental - The SDT will evaluate revision approaches and determine whether to develop requirements applicable to use of cloud for all CIP-defined systems (such as EACMS, PACS, BCS, etc.), or to develop incremental revisions to allow use of cloud for individual or groups of CIP-defined systems (for example, first revising the standards to allow for EACMS use of cloud services). The SDT will define a development plan for the project, giving particular consideration for EACMS defined systems as a top priority for revision because the existing CIP language prevents adoptions of security solutions with greater visibility, detection, correlation, analytics, and responsiveness available using cloud services.

- Auditability and use of third-party certifications – the SDT will set out requirement language to allow the use of independent third-party certifications/attestations to support auditability of the new or revised requirements and will incorporate language in the standard(s) as needed to clarify their use. Accepting independent third-party security assurance certifications/ attestations such as FedRAMP, SOC, ISO, or others is a valuable opportunity to set a high security standard for CSPs, recognize the rigor and cloud-security specific nature of such certifications, streamline the adoption and compliance demonstration process for regulated Entities, and support CIP auditor focus on assessing the power and utility operations and governance.

- Timing – the current CIP language applicable to assets that contain high and medium BES Cyber Systems includes or implies physical hardware that must reside within physical security perimeter (PSP), which is preventing adoption of cloud services that benefit security (i.e. security event monitoring solutions) and reliability (i.e. predictive maintenance solutions) today. The revised or new standard(s) is to be delivered in a timely manner and completed for submittal to FERC 12-18 months from the start of the SDT deliberations. As well, the implementation plan is to allow the possibility for early adoption ahead of any proposed enforceability date.

- Flexibility - The SDT may, as an alternative to a new or revised standard(s), propose equally efficient and effective means to meet the objectives. The drafting team may choose not to write standards and instead choose an alternate vehicle to allow for use of cloud services for CIP-regulated systems.

The following may serve as supporting documents for the SDT:

- SITES BES Operations in the Cloud whitepaper (pending publication)
- IEEE Practical Adoption of Cloud Computing in Power Systems- Drivers, Challenges, Guidance, and Real-world Use Cases

Requested information

• NERC in an informational filing to FERC in December 2021 identified the following areas of interest as potential educational topics about cloud environments, associated risks, and the risk mitigation measures when considering the new requirements:
  • Quality of Service and Resilience
  • Data Residency
  • Evaluation Criteria for Selection of Cloud Service Providers
  • Registered Entities Conducting Risk Assessments
  • Security Responsibilities
  • Compliance Oversight and Audit Processes

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Responsible Entities that implement CIP-regulated workloads in the cloud will incur costs related to compliance program revisions.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator
Do you know of any consensus building activities[6] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This SAR was informally shared with a wide network of stakeholders across industry to gather feedback. Updates were made to refine the SAR content based on that feedback. Respondents support development of this SAR and its submittal to NERC.
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)?
This project has the potential to impact current versions of the following NERC CIP Standards: CIP-002, CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011, CIP-012, CIP-013, CIP-014. This project also has the potential to impact Project 2016-02, Project 2023-03, Project 2021-03. As well, additional SARs may be in development on related topics (e.g. Revisions to appropriate CIP Standards to include Multi-factor Cloud-based Authentication services.)
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.

[6] 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
No

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

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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	None identified

For Use by NERC Only

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

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Project 2023-05 Modifications to FAC-001 and FAC-002

Action

Appoint chair, vice chair, and members to the Project 2023-05 Modifications to FAC-001 and FAC-002 drafting team (DT).

Background

The NERC System Performance Impacts of Distributed Energy Resources Work Group (SPIDERWG) evaluated the current body of NERC Reliability Standards and the requirements within those standards for distributed energy resource (DER) applicability and effectiveness with increasing penetrations of DER. This review is housed in the SPIDERWG White Paper: *NERC Reliability Standards Review*. The review occurred between 2018 and 2022, culminating in a handful of Standard Authorization Requests (SARs), including the SARs for FAC-001-4 and FAC-002-4. Both standards were identified as needing refinement to ensure that the reliability at the transmission to distribution interface (T-D interface) is maintained.

At its May 17, 2023 meeting, the Standards Committee (SC) accepted the FAC-001-4 and FAC-002-4 SARs and authorized soliciting members for the DT. The formal comment period and the solicitation for the DT member period ran from August 09 – September 27, 2023, which was extended due to a lack of industry nominations.

Summary

NERC received 10 nominations from industry. NERC staff recommends that the SC appoint all 10 nominees to the DT, as they all have the requisite background, experience, and skills necessary for membership.

Project 2021-03 CIP-002

Action

Appoint additional members to the Project 2021-03 CIP-002 Drafting Team (DT), as recommended by NERC staff.

Background

Project 2021-03 currently has five assigned Standard Authorization Requests (SARs):

- 2016-02 SAR – [Transmission Owner Control Centers (TOCC)] - Evaluate the categorization of TOCCs performing the functional obligations of a Transmission Operator, specifically those that meet medium impact criteria.
- CIP-002 and CIP-014 – By modifying the standards to replace/update language with regards to "critical to the derivation of the Interconnection Reliability Operating Limits (IROLS) to appropriately identify facilities."
- CIP-002 Communication Protocol Converters – Include the identification of communication protocol converters and the relationship to the exception in Section 4.2.3 in CIP-002.
- Modifications to CIP-002 – To ensure all BES Cyber Systems' associated Cyber Assets (CA) are identified for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those CA. Identification and categorization of these Cyber Assets supports appropriate protection against compromises. Without an accurate inventory of associated Cyber Assets, registered entities may fail to deploy appropriate controls to these Cyber Assets, which may lead to misoperation or instability in the BES.
- CIP-002-5.1a Criterion 1.3 Revision SAR – Seeks to add Criterion 2.6 to the list of Criteria in Criterion 1.3 in Attachment 1 of CIP-002-5.1a. This project will require the TOP to categorize its BES Cyber System(s) as high impact that meets Criterion 2.6, as is also required of the BA and GOP in Criterion 1.2 and 1.4. By including Criterion 2.6 in Criterion 1.3, the TOP's BES Cyber Systems(s) will be appropriately categorized as high impact for Transmission Facilities at a single station or substation location that is identified as critical to the derivation of IROLs and their associated contingencies.

The Standards Committee (SC) authorized solicitation for a SDT to conduct a field test and assigned a portion of the Project 2016-02 SAR related to TOCC to the SDT on March 17, 2021. The solicitation for the SDT occurred from March 22, 2021 — April 27, 2021. At the May 19, 2021 meeting, the SC appointed the chair, vice chair, and members to the Project 2021-03 CIP-002 SDT.

The SC approved the Project 2021-03 Field Test Plan on November 17, 2021. Three field tests were conducted in 2022, and the final report was posted to the project page in January 2023. Since then, the SDT has posted a draft of the revised CIP-002 standard for informal and formal

comment and initial ballot. On July 19, 2023, the SC authorized solicitation of additional drafting team members to supplement to bring additional expertise to the team.

Summary

From July 20 – August 18, 2023, NERC solicited nominations for supplemental volunteers to serve on the DT. NERC staff received four nominations from industry professionals and recommended three individuals, as they have the requisite background, experience, and skills necessary for membership in the DT.

Project 2020-02 Modifications to PRC-024 (Generator Ride-through) Waiver

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2020-02:

- Initial formal comment and ballot period reduced from 45 days to as few as 25 calendar days, with ballot pools formed in the first 10 days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 days of the comment period (Sections 4.7 and 4.9)
- Additional formal comment and ballot period (s) reduced from 45 days to as little as 15 days, with ballot conducted during the last 10 days of the comment period. (Sections 4.9 and 4.12)
- Final ballot reduced from 10 days to five calendar days. (Section 4.9)

Background

The SAR ensures generators remain connected to the bulk power system (BPS) during system disturbances. Specifically, this SAR focuses on the generator protection and control systems that can result in the reduction or disconnection of generating resources during these events. The SAR also ensures that protection or controls that fail to ride through system events are analyzed, addressed with a corrective action plan (if possible), and reported to necessary entities for situational awareness. However, those items are now covered within Project 2023-02. From a risk-based perspective, the goal of the standard is to mitigate the ongoing and systemic performance issues identified across multiple Interconnections and across many disturbances analyzed by NERC and the Regions. These issues have been identified in Inverter-Based Resources (IBR) and synchronous generators, with many causes of tripping entirely unrelated to voltage and frequency protection settings as dictated by the currently effective version of PRC-024.

At the April 19, 2023 meeting, the Standards Committee (SC) accepted the most recent revised SAR submitted by the Project 2020-02 Standard Drafting Team.

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 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.

FERC Order 901 directs the development of new or modified reliability standards that include new requirements for disturbance monitoring, data sharing, post-event performance validation, and correction of IBR performance. This set of directives from the report comprises the first three sets of Standards Projects that must be completed and filed with FERC. This first set (disturbance monitoring data sharing and post-event performance validation and correction of IBR performance) must be filed with FERC by November 4, 2024.

NERC Standards Development has identified three active projects (2020-02, 2021-04, and 2023-02) that are directly impacted by these associated FERC directives. Project 2020-02 DT leadership and NERC staff request that the SC approve a waiver for specific provisions of the SPM regarding the length of comment periods and ballots in order to meet the November 2024 development deadline for 2020-02 as established by FERC.

Summary

Project 2020-02 DT leadership and NERC staff recommend that the SC shorten the initial formal comment and ballot period from 45 days to as few as 25 days and any additional formal comment and ballot period(s) from 45 days to as few as 15 days. In addition, Project 2020-02 DT leadership and NERC staff recommend that the SC shorten the final ballot from 10 days to 5 days.

Project 2023-02 Analysis and Mitigation of BES Inverter-Based Resource Performance Issues Waiver

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2023-02:

- Initial formal comment and ballot period reduced from 45 days to as few as 25 calendar days, with ballot pools formed in the first 10 days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 days of the comment period (Sections 4.7 and 4.9)
- Additional formal comment and ballot period (s) reduced from 45 days to as little as 15 days, with ballot conducted during the last 10 days of the comment period. (Sections 4.9 and 4.12)
- Final ballot reduced from 10 days to five calendar days. (Section 4.9)

Background

The project addresses the reliability-related need by requiring analysis and mitigation of unexpected or unwarranted protection and control operations from Invert-Based Resources (IBRs). This includes any types of protections and controls that result in abnormal performance issues within the plant, including abnormal performance resulting in anomalous behavior of active power output from the facility during events. The SAR focuses on revisions to PRC-004-6 and should be applicable to all Bulk Electric System (BES) IBR generating resources, including battery storage.

At the January 25, 2023 meeting, the Standards Committee (SC) accepted the Standard Authorization Request (SAR) that was submitted by the Inverter-Based Resource Performance Subcommittee and authorized soliciting members for the Standard Drafting Team (SDT). The informal comment period and the solicitation for the drafting team members ran from February 22–March 23, 2023. The SDT was appointed at the June 21, 2023 SC meeting. During the October SC meeting, the SC accepted the redlined SAR.

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.

FERC Order 901 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. This set of directives from the report comprises the first of three standards projects that must be completed and filed with FERC. This first set (disturbance monitoring data sharing and post-event performance validation and correction of IBR performance) must be filed with FERC by November 4, 2024.

NERC Standards Development has identified three active projects (2020-02, 2021-04, and 2023-02) that are directly impacted by these associated FERC directives. Project 2023-02 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 2024 development deadline for 2023-02 as established by FERC.

Summary

Project 2023-02 DT leadership and NERC staff recommend that the SC shorten the initial formal comment and ballot period from 45 days to as few as 25 days and any additional formal comment and ballot period(s) from 45 days to as few as 15 days, In addition, Project 2023-02 DT leadership and NERC staff recommend shortening the final ballot from 10 days to 5 days.

Project 2021-04 Modifications to Disturbance Monitoring and Reporting Requirements

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2021-04:

- Additional formal comment and ballot period (s) reduced from 45 days to as little as 15 days, with ballot conducted during the last 10 days of the comment period. (Sections 4.9 and 4.12)
- Final ballot reduced from 10 days to five calendar days. (Section 4.9)

Background

The Project 2021-04 drafting team (DT) was charged with addressing two Standard Authorization Requests (SARs) related to PRC-002, to be addressed in two separate phases. The first SAR was submitted by Glencoe Light, who sought clarification of notifications and data requirements. The second SAR was submitted by the NERC Inverter-based Resource Performance Task Force (IRPTF). In its March 2020 white paper, *IRPTF Review of NERC Reliability Standards White Paper*, the IRPTF identified issues with PRC-002-2 that should be addressed.

At the Standards Committee (SC) January 20, 2021 meeting, the SC accepted both PRC-002 SARs referenced above and authorized soliciting for members for the SAR DT. At the September 23, 2021 meeting, the SC appointed chair, vice chair, and members to the Project 2021-04 Modifications to PRC-002 SAR DT. At its January 19, 2022 meeting, the SC accepted the revised SARs, authorized drafting revisions to the Reliability Standards identified in the SARs and appointed the SAR DT as the project DT.

The DT completed the first phase of work to address the Glencoe Light SAR in winter 2023 with the development of Reliability Standard PRC-002-4.

After much debate, the DT strongly believes that to address the needs identified in the IRPTF SAR, a new standard for monitoring requirements for Inverter-Based Resources (IBRs) should be created instead of revising PRC-002. As such, the DT submitted a revised SAR for SC approval on April 19, 2023. At that meeting, SC authorized drafting revisions to the Reliability Standards identified in the SAR, i.e., to create a new standard (PRC-028-1) to address needs identified in the IRPTF SAR and to make minor revisions to PRC-002 as necessary to align with the new standard.

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 government 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.

FERC Order 901 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. This set of directives from the report comprises the first of three sets of Standards Projects that must be completed and filed with FERC. This first set (disturbance monitoring data sharing and post-event performance validation and correction of IBR performance) must be filed with FERC by November 4, 2024.

NERC Standards Development has identified three active projects (2020-02, 2021-04, and 2023-02) that are directly impacted by these associated FERC directives. Project 2021-04 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 2024 development deadline for 2021-04 as established by FERC.

Summary

Project 2021-04 DT leadership and NERC staff recommend that the SC shorten additional formal comment and ballot period(s) from 45 days to as few as 15 days. NERC staff is only recommending this reduction for additional comment and ballot period(s) because initial ballot was completed August 1 – September 14, 2023. In addition, Project 2021-04 DT leadership and NERC staff recommend that the final ballot be shortened from 10 days to five days.

Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2023-07 Transmission System Planning Performance Requirements for Extreme Weather:

- Initial formal comment and ballot period were reduced from 45 days to as few as 25 days. (Sections 4.9 and 4.12)
- Additional formal comment and ballot period(s) reduced from 45 days to as few as 15 calendar days, with ballot(s) conducted during the last five days of the comment period. (Sections 4.9 and 4.12)
- Final ballot period was reduced from 10 days to as few as five calendar days. (Section 4.9)

Background

Section 16.0 of the SPM allows the Standards Committee to waive any provision in the SPM for good cause, including for the following reasons:

> *Where the Standards Committee 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.*

On June 15, 2023, FERC issued FERC Order 896, directing NERC to develop a new or modified Reliability Standard to address a need for long-term planning requirement(s) for extreme heat and cold weather events. Specifically, FERC directed NERC to develop modifications to Reliability Standard TPL-001-5.1 or a new Reliability Standard, to require the following: (1) development of benchmark planning cases based on major prior extreme heat and cold weather events and/or meteorological projections; (2) planning for extreme heat and cold weather events using steady state and transient stability analyses expanded to cover a range of extreme weather scenarios including the expected resource mix's availability during extreme heat and cold weather conditions, and including the wide-area impacts of extreme heat and cold weather; and (3) development of corrective action plans that mitigate any instances where performance requirements for extreme heat and cold weather events are not met. In addition to these directives, FERC directed NERC to modify an existing or create a new Reliability Standard by December 2024.

Summary

Given the stage of the directed due date of December 2024, the drafting team needs flexibility to condense the ballot and comment periods necessary to meet this due date while following the NERC processes therefore Project 2023-07 DT leadership and NERC staff recommend that the SC shorten the initial formal comment and ballot period from 45 days to as few as 25 days and any additional formal comment and ballot period(s) from 45 days to as few as 15 days. In

addition, Project 2023-07 DT leadership and NERC staff recommend shortening the final ballot from 10 days to 5 days.

Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2021-07:

- Additional formal comment and ballot period(s) reduced from 45 days to as little as 10 days, with ballot conducted concurrently during the last 5 days of the comment period. (Sections 4.9 and 4.12)

Background

As stated in the SAR, the primary purpose of this project is intended to address reliability related findings from FERC, NERC, and Regional Entity Joint Staff Inquiry into the February 2021 Cold Weather Grid Operations (joint inquiry). From February 8 - 20, 2021, extreme cold weather and precipitation caused large numbers of generating units to experience outages, derates, or failures to start, resulting in energy and transmission emergencies (referred to as "the Event"). The total Event firm load shed was the largest controlled firm load shed event in U.S. history and was the third largest in quantity of outaged megawatts (MW) of load after the August 2003 northeast blackout and the August 1996 west coast blackout. The Event was most severe from February 15 - February 18, 2021, and it contributed to power outages affecting millions of electricity customers throughout the regions of ERCOT, SPP, and MISO South. Additionally, the February 2021 event is the fourth cold weather event in the past 10 years that jeopardized bulk-power system reliability.

Standards development under Project 2021-07 proceeded in two phases in accordance with a directive by the NERC Board of Trustees issued at its November 2021 meeting. Work under the first phase completed in September 2022 with the development of Reliability Standards EOP-012-1 and EOP-011-3 in 2022. Work under the second phase completed in September 2023 with the development of Reliability Standards EOP-011-4 and TOP-002-5.

On February 16, 2023, shortly before the first ballot on the phase two standards, FERC issued an order approving Reliability Standards EOP-011-3 and EOP-012-2 while directing five areas for additional revisions. FERC directed NERC to submit a revised EOP-012 standard by February 2024.[1]

NERC Standard Processes Manual Section 16.0 Waiver provides as follows:

> The Standards Committee 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 government that involves the reliability of the Bulk Electric System or cyber attack on the Bulk Electric System;

[1] *Order Approving Extreme Cold Weather Reliability Standards EOP-011-3 and EOP-012-2 and Directing Modification of Reliability Standard EOP-012-1,* 182 FERC ¶ 61,094 (2023) (February 16, 2023 Order), available here.

- Where necessary to meet regulatory deadlines;
- Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
- Where the Standards Committee 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.

Due to the issuance of FERC's February 16, 2023 Order directing further revisions to EOP-012 by February 2024, the Project 2021-07 drafting team was delayed in the planned development timeline for the standards addressing the phase 2 recommendations of the February 2021 joint inquiry report.

In August 2023, the Standards Committee approved a Waiver under Section 16.0 of the Standard Processes Manual to shorten comment periods from 45 to as few as 25 days, with a ballot and non-binding poll during the last 10 days, and to shorten the final ballot from 10 days to 5 days.

Due to the recent failed additional ballot for draft standard EOP-012-2, and the Commission's February 2024 deadline, the Project 2021-07 SDT leadership and NERC staff request that the SC consider a waiver of these provisions for EOP-012-2 to shorten the comment period further. This is necessary for the drafting team to have a second additional comment and ballot period to develop a consensus standard by the February 2024 FERC deadline.

Summary

SDT leadership and NERC staff recommend shortening the additional formal comment and ballot period(s) for Project 2021-07 from 45 days to as few as 10 days, with a ballot and non-binding poll concurrent during the last 5 days of the comment period.

Project 2023-03 Internal Network Security Monitoring (INSM)

Action

Authorize initial posting of proposed Reliability Standard CIP-007-X and the associated Implementation Plan for a 35-day formal comment period, with ballot pool formed in the first 25 days and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for Internal Network Security Monitoring (INSM) of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues. In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC is conducting the study, which will be filed with FERC by January 18, 2024.

The Standards Committee (SC) accepted the revised SAR at its August 23, 2023 meeting. At that same meeting, the SC authorized drafting of the Reliability Standard(s) identified in the SAR and issued a waiver of Sections 4.7, 4.9, and 4.13 as they relate to the minimum required length for comment periods and ballots in order to meet the regulatory deadline established by FERC.

The Quality Review (QR) was performed from November 20 to November 29, 2023. The QR Team consisted of Sharon Koller (ATC), Jay Cribb (Southern Co.), Michaelson Buchanan (NERC Senior CIP Assurance Advisor, Compliance Assurance), Holly Peterson (NERC Compliance Assurance Manager), Davis Jelusich (NERC CIP Assurance Advisor), Sushil Subedi (NERC CIP Assurance Advisor), Lauren Perotti (NERC Legal), Sarah Crawford (NERC Legal) and Linda Jenkins (NERC Senior Standards Development Administrator).

Summary

NERC staff recommends that the SC authorize a 35-day formal comment period, with ballot pool formed in the first 25 days and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 10 days of the comment period.

Standard Development Timeline

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

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023

Anticipated Actions	Date
35-day formal comment period with ballot	12/14/2023 – 1/17/2024
XX-day formal comment period with additional ballot	TBD
XX-day final ballot	TBD
Board adoption	TBD

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

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

Term(s):

None.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 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 Special Protection System (SPS) where the SPS 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-X:

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

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

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

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

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

5. Effective Date: See Implementation Plan for CIP-007-X.

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-X Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

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

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

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-X Table R2 – 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	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X 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-X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

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

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X 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-X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System 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-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X 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-X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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 Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, 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.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – Internal Network Security Monitoring (INSM)* to increase the probability of detecting an attack that has bypassed other security controls. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment].*

M6. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – INSM* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.	Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R1. (R1)
R2.	The Responsible entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	included the applicable items in CIP-007-X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	or revised within the timeframe specified in the plan. (2.4)
R3.	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)
R4.	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented one or more	The Responsible Entity did not implement or document one or more

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access, but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar	process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			months of the last password change. (5.6)	obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)
R6.	The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).	The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).	The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3). OR The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices,	The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6). OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			and network communications using data from Part 6.2 (6.4). OR The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).	The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1). OR The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).

C. Regional Variances

None.

D. Associated Documents

None.

Version History

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

			communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-X. Docket No. RM15-14-000	
X	06/2023	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on xx/xx/xx. Revised version addresses Order No. 887 related to Internal Network Security Monitoring.

Standard Development Timeline

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

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023

Anticipated Actions	Date
35-day formal comment period with ballot	12/14/2023 – 1/17/2023
XX-day formal comment period with additional ballot	TBD
XX-day final ballot	TBD
Board adoption	TBD

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

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

Term(s):

None.

A. Introduction

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

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

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

~~3.~~4. **Applicability:**

~~3.1.~~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.

~~3.1.1~~4.1.1 **Balancing Authority**

~~3.1.2~~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:

~~3.1.2.1~~4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

~~3.1.2.1.1~~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

~~3.1.2.1.2~~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.

~~3.1.2.2~~4.1.2.2 Each Special Protection System (SPS) ~~or Remedial Action Scheme (RAS)~~ where the SPS ~~or RAS~~ is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.1.2.3~~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.

~~3.1.2.4~~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.

~~3.1.3~~4.1.3 **Generator Operator**

~~3.1.4~~4.1.4 **Generator Owner**

~~3.1.5~~4.1.5 **Interchange Coordinator or Interchange Authority**

~~3.1.6~~4.1.6 **Reliability Coordinator**

~~3.1.7~~4.1.7 **Transmission Operator**

~~3.1.8~~4.1.8 **Transmission Owner**

~~3.2.~~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.

~~3.2.1~~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:

~~3.2.1.1~~4.2.1.1 Each UFLS or UVLS System that:

~~3.2.1.1.1~~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

~~3.2.1.1.2~~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.

~~3.2.1.2~~4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.3~~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.

~~3.2.1.4~~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.

~~3.2.2~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

~~3.2.3~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-X:

~~3.2.3.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~3.2.3.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~3.2.3.3~~4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~3.2.3.4~~4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~3.2.3.5~~4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

~~4.~~5. **Effective Date:** See Implementation Plan for CIP-007-~~6~~X.

~~5. **Background:** Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

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

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

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

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

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

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

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

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

~~"Applicable Systems" Columns in Tables:~~

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

- **~~High Impact BES Cyber Systems –~~** ~~Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~
- **~~Medium Impact BES Cyber Systems –~~** ~~Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- **~~Medium Impact BES Cyber Systems at Control Centers –~~** ~~Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- **~~Medium Impact BES Cyber Systems with External Routable Connectivity –~~** ~~Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- **~~Electronic Access Control or Monitoring Systems (EACMS) –~~** ~~Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- **~~Physical Access Control Systems (PACS) –~~** ~~Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

- ~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X~~6~~ Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

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

CIP-007-~~6~~ X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~6~~ X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

~~M1.~~M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~ X Table R2 – 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	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES -Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

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

~~M2.~~M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

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

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

~~M3.~~M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

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

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

~~M4.~~M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems- and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~6~~ XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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 Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, 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.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – Internal Network Security Monitoring (INSM)* to increase the probability of detecting an attack that has bypassed other security controls. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment].*

M6. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – INSM* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods

6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

6.4	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.

6.5	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.	Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.

6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary. ~~b R6, Part~~

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R1. (R1)
R2.	The Responsible entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	included the applicable items in CIP-007-~~6~~ X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	or revised within the timeframe specified in the plan. (2.4)
R3.	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)
R4.	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented one or more	The Responsible Entity did not implement or document one or more

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5)~~	~~documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)~~ OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).	The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).	The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3). OR The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2 (6.4). OR The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).	The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6). OR The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).

C. Regional Variances

None.

D. Associated Documents

None.

Version History

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

			communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-~~6~~X. Docket No. RM15-14-000	
X	06/2023	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on xx/xx/xx. Revised version addresses Order No. 887 related to Internal Network Security Monitoring.

~~Guidelines and Technical Basis~~

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

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

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

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

~~Requirement R1:~~

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

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

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

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

- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

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

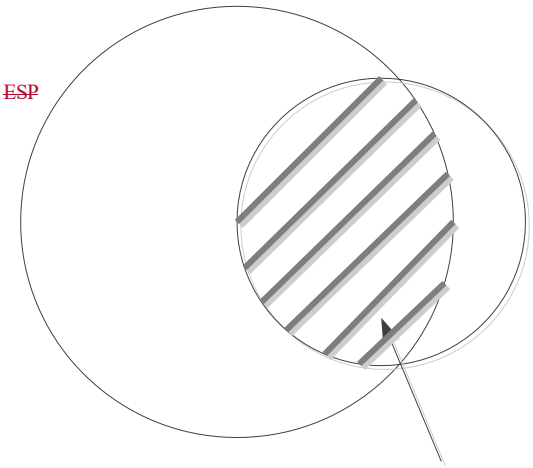
~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control.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

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

Location of Nonprogrammable Communication Components

PSP

ESP



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an

"install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

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

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

The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock

~~starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the~~

~~Cyber Asset's baseline.~~

~~Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the~~

~~Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch~~

~~Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

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

~~**2.1.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can~~

~~document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

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

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

Requirement R3:

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

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

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

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

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

Requirement R4:

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

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

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

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

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

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

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

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

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

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

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

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

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

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

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

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

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

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

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

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

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

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

~~Rationale:~~

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

~~Rationale for Requirement R1:~~

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

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

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

~~Rationale for Requirement R2:~~

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

~~Rationale for Requirement R3:~~

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

~~Rationale for Requirement R4:~~

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

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

~~Rationale for Requirement R5:~~

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

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

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

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

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

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

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

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

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

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standards Committee Charter Revisions

Action

Approve revisions to the Standards Committee Charter for submission to the NERC Board of Trustees (Board).

Background

At its meeting on October 10, 2022, the Board recommended the following revisions to the Standards Committee (SC) Charter to allow expanded use of the Standards Committee Executive Committee (SCEC) to keep progress advancing on projects in between scheduled meetings of the full SC consistent with an open and transparent process, including revisions to address the following:

- Expanding the authority of the SCEC to authorize administrative actions (e.g., posting for supplemental drafting team nomination periods and posting for supplemental Standard Authorization Requests (SARs) for projects in active development);
- Expanding the authority of the SCEC to approve procedural actions relating to supplemental or revised SARs postings during the standard drafting phase, as well as the authority to allow shortened informal comment periods for such SARs;
- Clarifying that the chair and vice chair are voting members of the SCEC;
- Allowing for the election of up to seven members to the SCEC; and
- Clarifying that all actions of the SCEC must be open to the public; documented in meeting minutes, and reported out to the full SC at its next regularly scheduled meeting

Summary

The charter was revised in Chapter 7 to address the SPSEG recommendations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 14a
Standards Committee
December 13, 2023

Standards Committee Charter

Approved by the Standards Committee

TBD

RELIABILITY | RESILIENCE | SECURITY




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

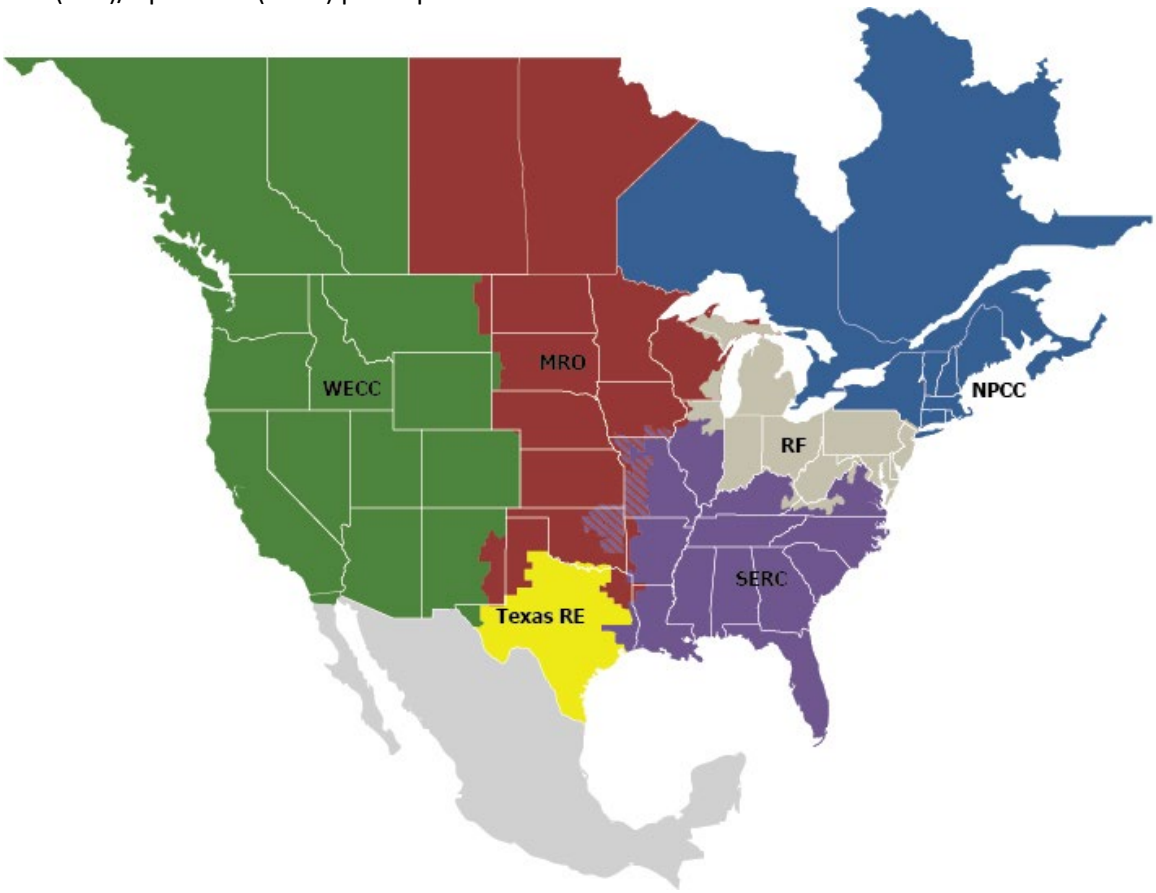
Table of Contents

Preface

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

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

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



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

Chapter 1: Purpose

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 establish 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.

Chapter 2: Reporting

The Committee reports and is accountable to the NERC Board of Trustees. The Committee members have the responsibility to keep the industry segments they represent informed regarding Reliability Standards matters. The NERC Board of Trustees shall approve amendments to this Charter pursuant to Section 1300 of the NERC Rules of Procedure.

Chapter 3: Overview and Functions

The Committee manages the NERC process to develop and maintain a comprehensive set of results-based Reliability Standards. Specifically, working together with NERC Standards Staff, the Committee has the following duties:

- Develop a long-term (multi-year) strategic vision describing the goals and direction for Reliability Standards development consistent with NERC's strategic and business plans.
- Coordinate with the Reliability Issues Steering Committee (RISC) to develop a Reliability Standards Development Plan (RSDP) prioritizing and aggressively pursuing work related to the purpose of the Committee.
- Assist to develop the RSDP, inclusive of preparing the initial posting for stakeholder comment.
- Establish and facilitate informal and formal collaborative, consensus building processes with stakeholder groups and NERC committees.
- Establish quality assurance and quality control processes to develop or modify Reliability Standards and applicable associated documents to align with the criteria established in the Standards Process Manual.
- Appoint, monitor and direct teams for work related to the Standards Process Manual (inclusive of, but not limited to, standard drafting teams) generally consisting of subject matter experts, a facilitator, a technical writer and compliance, legal and regulatory experts suitably equipped to address the desired reliability objectives.
- Receive and respond to decisions of appeals panels in accordance with the Reliability Standards process.
- Develop, maintain and implement a Standard Processes Manual ensuring the integrity of Reliability Standards development in a fair, balanced, open, and inclusive manner.
- Facilitate communication with regard to NERC Standards department and Standards Committee work, such as Reliability Standards under development and Standards Committee guiding documents.
- May consult with another NERC Committee for input to technical justification or alternate approaches to issues raised in a SAR.

Chapter 4: Membership

Segment Representation

The Committee membership consists of two members elected from each industry segment in accordance with Appendix 3B (*Procedures for Election of Members of the Standards Committee*) to the NERC Rules of Procedure. Each industry segment may establish its own rules for electing and replacing its SC representatives consistent with the following requirements:

Membership Requirements

No two persons employed by the same corporation or organization or an affiliate may serve concurrently as Committee members.

- Any Committee member with such a membership conflict shall notify the Committee secretary who will inform the Committee chair.
- Members impacted by a conflict, such as through a merger of organizations, may confer between themselves to determine which member should resign from the Committee and notify the Committee secretary and chair. If the impacted members do not resolve the conflict in a timely manner, the Committee chair shall notify all members of the affected industry segments of the need to resolve the conflict. If the membership conflict remains unresolved, the Committee chair shall take the conflict to the NERC Board of Trustees for resolution.
- Any Committee member aware of an unresolved membership issue shall notify the Committee chair.

Resignation from the Committee

Any member of the Committee who resigns from the Committee shall submit a written resignation to the Committee secretary and Committee chair.

- The Committee secretary shall facilitate election of a replacement member from the applicable industry segment to serve the remainder of the resigned member's term.
- If any member of the Committee fails to attend or send a proxy for more than two consecutive regularly scheduled meetings or conference calls, or more than two e-mail ballots between regularly-scheduled meetings, the Committee chair shall send a written notice to that member requesting the member either: (i) resign; or (ii) provide an explanation of the member's absences. If the member does not provide a written response within 30 calendar days of the date of the written notice, lack of response shall be deemed a resignation

Committee Member Change of Employment

- Any Committee member who leaves one organization and is subsequently employed by another organization in the same industry segment may retain the membership position.
- If a Committee member changes employment to an organization in a different industry segment, that Committee member shall resign from the Committee no later than the date of the employment change. The resignation letter shall be addressed to the Committee chair who will provide the letter to the Committee secretary and request an election to fill the vacant position. In the absence of a formal resignation, the Committee member will be deemed to have resigned as of the date the Committee chair or secretary becomes aware of the employment change.

Membership Terms

Committee members shall serve a term of two years without limitation to the number of terms the members may

serve, with members' terms staggered so half of the members (one per segment) is elected each year by industry segment election. Membership terms start on January 1 of each year.

Vacancies Caused by Election of Officers

The vacancies in the industry segments and/or Canada representation created by selection of the chair and vice chair shall be filled at the next annual election of Committee representatives. When a representative is elected to serve as the chair or vice chair during the second year of a two year term, the representative elected to fill the vacancy shall serve a one year term.

NERC Director of Standards or Designee

Acts as a non-voting Committee member to represent NERC's position on agenda items with the assistance of NERC Standards Staff.

Chapter 5: Officers

Selection

Prior to the annual election of Committee representatives in odd numbered years, the Committee members shall select a chair and vice chair from among their membership by majority vote. The chair and vice chair cannot represent the same industry segment. Approximately 150 calendar days prior to the end of each term, a nominating committee shall solicit nominations for chair and vice chair. The nominating committee shall consult with the NERC Board of Trustees' SC liaison on the nominations received.

No less than ten calendar days before the election date, the nominating committee shall provide to the Committee members the qualifications of the chair and vice chair nominees. At the time of the election, the Committee can accept nominations from the floor. Following the election, the successful candidates shall be presented to the NERC Board of Trustees for approval. The chair and vice chair, upon assuming such positions, shall cease to act as representatives of the industry segments that elected them and thereafter be responsible for acting in the best interests of the Committee as a whole.

Terms

The term of office for the Committee chair and vice chair is two years without limit on the number of terms an officer may serve. A member of NERC staff serves as the Committee's non-voting secretary.

Voting

The Committee chair and vice chair are non-voting Committee members.

Duties of the Chair

In addition to the duties, rights and privileges discussed elsewhere in this document, the Committee chair:

- Presides over and provides general supervision of Committee and Executive Committee activities and meetings.
- Presides over all Committee meetings, including the nature and length of discussion, recognition of speakers, motions and voting.
- In concert with NERC Staff, schedules Committee meetings.
- Reviews all substitute or proxy representatives.
- Acts as Committee spokesperson at forums within and outside of NERC.
- Reports Committee activities to the NERC Board of Trustees and attends Board of Trustees meetings.
- Reports all views and objections when reporting on items brought to the Committee.
- Performs other duties as directed by the NERC Board of Trustees.
- Participates as a member of the Standing Committees Coordinating Group (SCCG).

Duties of the Vice Chair

The Committee vice chair acts as the Committee chair if requested by the chair (for brief periods of time) or if the chair is absent or unable to perform the chair's duties. If the chair resigns prior to the next scheduled election, the vice chair shall act as the chair until the Committee selects a new chair. The vice chair:

- Assists the Committee chair in managing Committee meetings, including the nature and length of discussion, recognition of speakers, motions, and voting.

- Attends meetings of the NERC Board of Trustees in the chair's absence.
- Participates as a member of the SCCG.

Duties of the Secretary

A member of NERC staff shall serve under the direction of the Committee officers as a non-voting secretary and has the responsibility to:

- Conduct the day-to-day operation and business of the Committee.
- Prepare, distribute and post notices of Committee meetings, record meeting proceedings, and prepare, distribute and post meeting minutes.
- Maintain a record of all Committee proceedings, including attendance, responses, voting records, and correspondence.
- Maintain Committee membership records.
- Offer newly elected Committee members onboarding training, in partnership with the Committee Chair and Vice Chair.

Chapter 6: Voting Members' Expectations and Responsibilities

Voting members manage the NERC process to develop and maintain a comprehensive set of results-based Reliability Standards. Voting members have the following expectation and responsibilities:

- Contribute to the Committee's work and success by, among other things, executing the Committee Strategic Work Plan.
- Have familiarity with the Standard Processes Manual and ensure all actions adhere to the processes within.
- Serve as subject matter expert representatives of their industry segments and represent their industry segments.
- Be knowledgeable of NERC Reliability Standards development activities.
- Express opinions on behalf of their segments.
- Respond promptly to all Committee requests for attendance, reviews, comments and voting.
- Assist with outreach on the Reliability Standards development process.
- When unable to attend a Committee meeting notify the secretary and identify a proxy as described under Section 9. Meetings, sub section 9. Proxies, infra. The member shall instruct the proxy on the role and responsibilities.
- Duty of Care: Use due care and are diligent with respect to managing and administering the affairs of NERC and the Committee. This duty of care is generally thought to have two components: (i) the time and attention devoted to NERC's mission, and (ii) the skill and judgment reflected in the Committee's decisions.
- Duty of Loyalty: The duty of loyalty requires the members to faithfully promote the mission of NERC and the Committee, rather than their own or their entities' interests. This duty includes compliance with NERC's policies on conflicts of interest.
- Duty to Adhere to High Ethical Standards: The duty to adhere to applicable law and high ethical standards requires Committee members to devote themselves to ensuring they further NERC's stated objectives in compliance with legal requirements and high ethical standard

Chapter 7: Executive Committee

The Committee shall have an Executive Committee (SCEC) consisting of no less than five or up to seven members as follows:

- Chair;
- Vice Chair;
- Three to Five segment members as elected by the Committee.
  The segment members cannot represent the same industry segments the Committee officers previously represented, nor can any two of the segment members be from the same segment.

Each member of the SCEC is a voting member, including the Chair and Vice Chair.

The Executive Committee will be elected annually at the January Committee meeting. In the event of an SCEC vacancy before conclusion of the term, an election will be announced at the next regularly scheduled Committee meeting to be conducted at the following Committee meeting.

The Executive Committee is authorized by the Committee to act on its behalf between regular meetings on matters where urgent actions are crucial and full Committee discussions are not practical. Each meeting of the SCEC acting on the Committee's behalf shall be open to all interested parties, subject to any preregistration requirements, and publicly noticed. The Committee shall be notified of such urgent actions taken by the SCEC within a week of such actions. These actions shall also be included in the minutes of the next open meeting.

Ultimate Committee responsibility resides with its full membership whose decisions cannot be overturned by the SCEC. The Committee retains the authority to ratify, modify, or annul SCEC actions.

Additionally, the Executive Committee shall have the authority to:

- Work with NERC Standards Staff to set agendas for Committee meetings.
- Act on the Committee's behalf to authorize solicitation of drafting team members, postings of SARs, Reliability Standards, and other Standards-related documents for both new and currently active standards development projects.
- Act on the Committee's behalf to authorize Section 16.0 Waivers to shorten usual process timelines.
- Provide advice and guidance to subcommittee chairs, as needed.
- Take any actions delegated by the full Committee.

Chapter 8: Subordinate Groups

The SC organizational structure will be aligned as described by the NERC Bylaws to support a superior-subordinate hierarchy.

The SC may establish subcommittees, working groups, and task forces as necessary. The SC will be the responsible sponsor of all subordinate subcommittees, working groups, or task forces that it creates, or that its subordinate subcommittees and working groups may establish.

Officers of subordinate groups will be appointed by the chair of the SC.

Subcommittees, working groups, and taskforces will conduct business in a manner consistent with all applicable sections of this Charter.

Subcommittees

The SC may establish subcommittees to which the SC may delegate some of SC's functions. The SC will approve the scope of each subcommittee it forms. The SC chair will appoint the subcommittee officers (typically a chair and a vice chair) for a specific term (generally two years). The subcommittee officers may be reappointed for an indefinite number of additional terms. The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the committee. The formation of a subcommittee, due to the permanency of the subcommittee, will be approved by the NERC Board.

Working Groups

The SC may delegate specific continuing functions to a working group. The SC will approve the scope of each working group that it forms. The SC chair will appoint the working group officers (typically a chair and a vice chair) for a specific term (generally two years). The SC will conduct a "sunset" review of each working group every year. The working group will be accountable for the responsibilities assigned to it by the SC or subcommittee and will, at all times, work within its assigned scope. The SC should consider promoting to a subcommittee any working group that is required to work longer than one term.

Task Forces

The SC may assign specific work to a task force. The SC will approve the scope of each task force it forms. The SC chair will appoint the task force officers (typically a chair and a vice chair). Each task force will have a finite duration, normally less than one year. The SC will review the task force scope at the end of the expected duration and at each subsequent meeting of the SC until the task force is retired. Action of the SC is required to continue the task force past its defined duration. The SC should consider promoting to a working group any task force that is required to work longer than one year.

Chapter 9: Meetings

Open Meetings

Committee meetings shall be open to all interested parties, subject to any preregistration meeting requirements included in the meeting announcement. Meeting notices shall describe the meeting's purpose and identify a readily available source for further information about the meeting. Only voting members may act on items before the Committee. The Committee secretary shall post meeting notices and agendas on the NERC website contemporaneously with distribution to Committee members. The Committee secretary shall publicly post final minutes of Committee meetings on the NERC website within five business days of Committee approval.

General Requirements

The Committee shall hold meetings as needed and may use conference calls or e-mail to conduct its business.

Notice

The Committee secretary shall announce regularly scheduled meetings with a written notice (letter, facsimile, or e-mail) to all Committee members not less than ten nor more than sixty calendar days prior to the meeting date.

Agenda

The secretary shall provide an agenda with a written notice (letter, facsimile, or e-mail) for Committee meetings no less than five business days before a proposed meeting.

- The agenda shall include, as necessary, background material for agenda items requiring a decision or vote. The secretary shall post the agenda on the NERC website the same day it is distributed to Committee members.
- Items not in the agenda that require a vote cannot be added at a meeting without the unanimous consent of the members present. If such a matter arises, it may also be deferred to the next meeting to allow Committee members to consult with their industry segments.

Parliamentary Procedures

In the absence of specific provisions in this Charter, the Committee shall conduct its meetings guided by the most recent edition of *Robert's Rules of Order, Newly Revised*.

Quorum

A quorum requires two-thirds of the Committee voting members.

Voting

Voting may take place during regularly scheduled meetings or through electronic means.

- All Committee actions shall be approved upon receipt of the affirmative vote of a majority of the members present and voting at a meeting with a quorum present, with the exception of revisions to the Standard Processes Manual and the Committee Charter which can be approved only upon receipt of the affirmative vote of two-thirds of the members present and voting at a meeting with a quorum present.
- Each individual member's vote for each action taken shall be included in the minutes of each meeting, unless the vote is unanimous with no abstentions.

Actions without a Meeting

The Committee may act by mail or e-mail ballot without a regularly scheduled meeting. A majority of the members participating in the voting is required to approve any action. A quorum for actions without a meeting is two-thirds of

Committee members. The Committee chair or four members (each from a different industry segment) may initiate the request for an action without a meeting. The secretary shall post a notice on the NERC website and provide Committee members a written notice (letter, facsimile, or e-mail) of the subject matter for action not less than three business days prior to the date on which the vote is to be counted. The secretary shall both distribute a written notice to the Committee (letter, facsimile, or e-mail) of the results of such action within five business days following the vote and post the results on the NERC website. The secretary shall keep a record of all responses (e-mails, facsimiles, etc.) from the Committee members with the Committee minutes.

Waivers

From time to time it may be necessary to develop a new or modified Reliability Standard, definition, Variance, Interpretation, or implementation plan under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn't sufficient time to follow all the steps in the normal Reliability Standards development process. The Standards Committee may waive any of the provisions contained in the Standard Processes Manual for good cause shown, but limited to the circumstances established in Section 16.0 of the Manual. A waiver request may be submitted to the Committee by any entity or individual. Prior to consideration of any waiver request, the Standards Committee must provide five business days' notice to stakeholders. This provision shall not be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

Proxies

A Committee member may designate a proxy. Proxies may attend and vote at Committee meetings provided the absent Committee member notifies in writing (letter, facsimile, or e-mail) the Committee chair, vice chair or secretary along with the reason(s) for the proxy. The member shall name the proxy representative and affiliation in the correspondence. No Committee member can serve as a proxy for another Committee member. The proxy must adhere to the Voting Members' Expectations and Responsibilities as described in Section 6, above.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 14a
Standards Committee
December 13, 2023

Standards Committee Charter

Approved by the Standards Committee

~~December 2021~~TBD

RELIABILITY | RESILIENCE | SECURITY




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

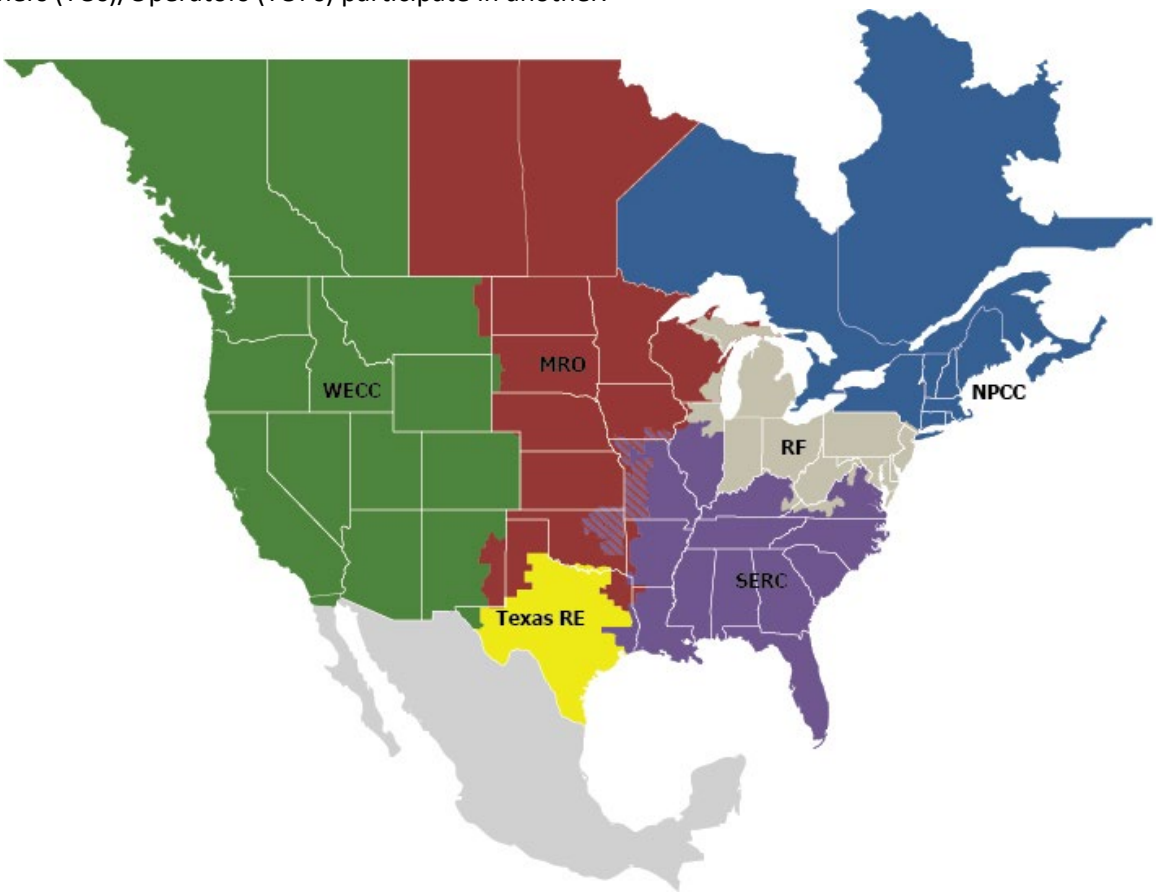
Table of Contents

Preface

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

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

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



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

Chapter 1: Purpose

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 establish 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.

Chapter 2: Reporting

The Committee reports and is accountable to the NERC Board of Trustees. The Committee members have the responsibility to keep the industry segments they represent informed regarding Reliability Standards matters. The NERC Board of Trustees shall approve amendments to this Charter pursuant to Section 1300 of the NERC Rules of Procedure.

Chapter 3: Overview and Functions

The Committee manages the NERC process to develop and maintain a comprehensive set of results-based Reliability Standards. Specifically, working together with NERC Standards Staff, the Committee has the following duties:

- Develop a long-term (multi-year) strategic vision describing the goals and direction for Reliability Standards development consistent with NERC's strategic and business plans.
- Coordinate with the Reliability Issues Steering Committee (RISC) to develop a Reliability Standards Development Plan (RSDP) prioritizing and aggressively pursuing work related to the purpose of the Committee.
- Assist to develop the RSDP, inclusive of preparing the initial posting for stakeholder comment.
- Establish and facilitate informal and formal collaborative, consensus building processes with stakeholder groups and NERC committees.
- Establish quality assurance and quality control processes to develop or modify Reliability Standards and applicable associated documents to align with the criteria established in the Standards Process Manual.
- Appoint, monitor and direct teams for work related to the Standards Process Manual (inclusive of, but not limited to, standard drafting teams) generally consisting of subject matter experts, a facilitator, a technical writer and compliance, legal and regulatory experts suitably equipped to address the desired reliability objectives.
- Receive and respond to decisions of appeals panels in accordance with the Reliability Standards process.
- Develop, maintain and implement a Standard Processes Manual ensuring the integrity of Reliability Standards development in a fair, balanced, open, and inclusive manner.
- Facilitate communication with regard to NERC Standards department and Standards Committee work, such as Reliability Standards under development and Standards Committee guiding documents.
- May consult with another NERC Committee for input to technical justification or alternate approaches to issues raised in a SAR.

Chapter 4: Membership

Segment Representation

The Committee membership consists of two members elected from each industry segment in accordance with Appendix 3B (*Procedures for Election of Members of the Standards Committee*) to the NERC Rules of Procedure. Each industry segment may establish its own rules for electing and replacing its SC representatives consistent with the following requirements:

Membership Requirements

No two persons employed by the same corporation or organization or an affiliate may serve concurrently as Committee members.

- Any Committee member with such a membership conflict shall notify the Committee secretary who will inform the Committee chair.
- Members impacted by a conflict, such as through a merger of organizations, may confer between themselves to determine which member should resign from the Committee and notify the Committee secretary and chair. If the impacted members do not resolve the conflict in a timely manner, the Committee chair shall notify all members of the affected industry segments of the need to resolve the conflict. If the membership conflict remains unresolved, the Committee chair shall take the conflict to the NERC Board of Trustees for resolution.
- Any Committee member aware of an unresolved membership issue shall notify the Committee chair.

Resignation from the Committee

Any member of the Committee who resigns from the Committee shall submit a written resignation to the Committee secretary and Committee chair.

- The Committee secretary shall facilitate election of a replacement member from the applicable industry segment to serve the remainder of the resigned member's term.
- If any member of the Committee fails to attend or send a proxy for more than two consecutive regularly scheduled meetings or conference calls, or more than two e-mail ballots between regularly-scheduled meetings, the Committee chair shall send a written notice to that member requesting the member either: (i) resign; or (ii) provide an explanation of the member's absences. If the member does not provide a written response within 30 calendar days of the date of the written notice, lack of response shall be deemed a resignation

Committee Member Change of Employment

- Any Committee member who leaves one organization and is subsequently employed by another organization in the same industry segment may retain the membership position.
- If a Committee member changes employment to an organization in a different industry segment, that Committee member shall resign from the Committee no later than the date of the employment change. The resignation letter shall be addressed to the Committee chair who will provide the letter to the Committee secretary and request an election to fill the vacant position. In the absence of a formal resignation, the Committee member will be deemed to have resigned as of the date the Committee chair or secretary becomes aware of the employment change.

Membership Terms

Committee members shall serve a term of two years without limitation to the number of terms the members may

serve, with members' terms staggered so half of the members (one per segment) is elected each year by industry segment election. Membership terms start on January 1 of each year.

Vacancies Caused by Election of Officers

The vacancies in the industry segments and/or Canada representation created by selection of the chair and vice chair shall be filled at the next annual election of Committee representatives. When a representative is elected to serve as the chair or vice chair during the second year of a two year term, the representative elected to fill the vacancy shall serve a one year term.

NERC Director of Standards or Designee

Acts as a non-voting Committee member to represent NERC's position on agenda items with the assistance of NERC Standards Staff.

Chapter 5: Officers

Selection

Prior to the annual election of Committee representatives in odd numbered years, the Committee members shall select a chair and vice chair from among their membership by majority vote. The chair and vice chair cannot represent the same industry segment. Approximately 150 calendar days prior to the end of each term, a nominating committee shall solicit nominations for chair and vice chair. The nominating committee shall consult with the NERC Board of Trustees' SC liaison on the nominations received.

No less than ten calendar days before the election date, the nominating committee shall provide to the Committee members the qualifications of the chair and vice chair nominees. At the time of the election, the Committee can accept nominations from the floor. Following the election, the successful candidates shall be presented to the NERC Board of Trustees for approval. The chair and vice chair, upon assuming such positions, shall cease to act as representatives of the industry segments that elected them and thereafter be responsible for acting in the best interests of the Committee as a whole.

Terms

The term of office for the Committee chair and vice chair is two years without limit on the number of terms an officer may serve. A member of NERC staff serves as the Committee's non-voting secretary.

Voting

The Committee chair and vice chair are non-voting Committee members.

Duties of the Chair

In addition to the duties, rights and privileges discussed elsewhere in this document, the Committee chair:

- Presides over and provides general supervision of Committee and Executive Committee activities and meetings.
- Presides over all Committee meetings, including the nature and length of discussion, recognition of speakers, motions and voting.
- In concert with NERC Staff, schedules Committee meetings.
- Reviews all substitute or proxy representatives.
- Acts as Committee spokesperson at forums within and outside of NERC.
- Reports Committee activities to the NERC Board of Trustees and attends Board of Trustees meetings.
- Reports all views and objections when reporting on items brought to the Committee.
- Performs other duties as directed by the NERC Board of Trustees.
- Participates as a member of the Standing Committees Coordinating Group (SCCG).

Duties of the Vice Chair

The Committee vice chair acts as the Committee chair if requested by the chair (for brief periods of time) or if the chair is absent or unable to perform the chair's duties. If the chair resigns prior to the next scheduled election, the vice chair shall act as the chair until the Committee selects a new chair. The vice chair:

- Assists the Committee chair in managing Committee meetings, including the nature and length of discussion, recognition of speakers, motions, and voting.

- Attends meetings of the NERC Board of Trustees in the chair's absence.
- Participates as a member of the SCCG.

Duties of the Secretary

A member of NERC staff shall serve under the direction of the Committee officers as a non-voting secretary and has the responsibility to:

- Conduct the day-to-day operation and business of the Committee.
- Prepare, distribute and post notices of Committee meetings, record meeting proceedings, and prepare, distribute and post meeting minutes.
- Maintain a record of all Committee proceedings, including attendance, responses, voting records, and correspondence.
- Maintain Committee membership records.
- Offer newly elected Committee members onboarding training, in partnership with the Committee Chair and Vice Chair.

Chapter 6: Voting Members' Expectations and Responsibilities

Voting members manage the NERC process to develop and maintain a comprehensive set of results-based Reliability Standards. Voting members have the following expectation and responsibilities:

- Contribute to the Committee's work and success by, among other things, executing the Committee Strategic Work Plan.
- Have familiarity with the Standard Processes Manual and ensure all actions adhere to the processes within.
- Serve as subject matter expert representatives of their industry segments and represent their industry segments.
- Be knowledgeable of NERC Reliability Standards development activities.
- Express opinions on behalf of their segments.
- Respond promptly to all Committee requests for attendance, reviews, comments and voting.
- Assist with outreach on the Reliability Standards development process.
- When unable to attend a Committee meeting notify the secretary and identify a proxy as described under Section 9. Meetings, sub section 9. Proxies, infra. The member shall instruct the proxy on the role and responsibilities.
- Duty of Care: Use due care and are diligent with respect to managing and administering the affairs of NERC and the Committee. This duty of care is generally thought to have two components: (i) the time and attention devoted to NERC's mission, and (ii) the skill and judgment reflected in the Committee's decisions.
- Duty of Loyalty: The duty of loyalty requires the members to faithfully promote the mission of NERC and the Committee, rather than their own or their entities' interests. This duty includes compliance with NERC's policies on conflicts of interest.
- Duty to Adhere to High Ethical Standards: The duty to adhere to applicable law and high ethical standards requires Committee members to devote themselves to ensuring they further NERC's stated objectives in compliance with legal requirements and high ethical standard

Chapter 7: Executive Committee

The Committee shall have an Executive Committee (SCEC) consisting of no less than five or up to seven members as follows:

- Chair;
- Vice Chair;
- Three to Five segment members as elected by the Committee.
  ~~, including the Committee officers plus three segment members, elected by the Committee.~~ The ~~three~~ segment members cannot represent the same industry segments the Committee officers previously represented, nor can any two of the segment members be from the same segment.

Each member of the SCEC is a voting member, including the Chair and Vice Chair.

The Executive Committee will be elected annually at the January Committee meeting. In the event of an SCEC vacancy before conclusion of the term, an election will be announced at the next regularly scheduled Committee meeting to be conducted at the following Committee meeting.

The Executive Committee is authorized by the Committee to act on its behalf between regular meetings on matters where urgent actions are crucial and full Committee discussions are not practical. Each meeting of the SCEC acting on the Committee's behalf shall be open to all interested parties, subject to any preregistration requirements, and publicly noticed. The Committee shall be notified of such urgent actions taken by the SCEC within a week of such actions. These actions shall also be included in the minutes of the next open meeting. ~~shall meet when necessary between regularly scheduled Committee meetings to conduct Committee business.~~

Ultimate Committee responsibility resides with its full membership whose decisions cannot be overturned by the SCEC. The Committee retains the authority to ratify, modify, or annul SCEC actions. ~~However, the SCEC shall not reverse the Committee's decisions.~~

Additionally, the Executive Committee shall have the authority to:

- Work with NERC Standards Staff to set agendas for Committee meetings.
- Act on the Committee's behalf to authorize solicitation of drafting team members, postings of SARs, Reliability Standards, and other Standards-related documents for both new and currently active standards development projects.
- Act on the Committee's behalf to authorize Section 16.0 Waivers to shorten usual process timelines.
- Provide advice and guidance to subcommittee chairs, as needed.
- Take any actions delegated by the full Committee.

Chapter 8: Subordinate Groups

The SC organizational structure will be aligned as described by the NERC Bylaws to support a superior-subordinate hierarchy.

The SC may establish subcommittees, working groups, and task forces as necessary. The SC will be the responsible sponsor of all subordinate subcommittees, working groups, or task forces that it creates, or that its subordinate subcommittees and working groups may establish.

Officers of subordinate groups will be appointed by the chair of the SC.

Subcommittees, working groups, and taskforces will conduct business in a manner consistent with all applicable sections of this Charter.

Subcommittees

The SC may establish subcommittees to which the SC may delegate some of SC's functions. The SC will approve the scope of each subcommittee it forms. The SC chair will appoint the subcommittee officers (typically a chair and a vice chair) for a specific term (generally two years). The subcommittee officers may be reappointed for an indefinite number of additional terms. The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the committee. The formation of a subcommittee, due to the permanency of the subcommittee, will be approved by the NERC Board.

Working Groups

The SC may delegate specific continuing functions to a working group. The SC will approve the scope of each working group that it forms. The SC chair will appoint the working group officers (typically a chair and a vice chair) for a specific term (generally two years). The SC will conduct a "sunset" review of each working group every year. The working group will be accountable for the responsibilities assigned to it by the SC or subcommittee and will, at all times, work within its assigned scope. The SC should consider promoting to a subcommittee any working group that is required to work longer than one term.

Task Forces

The SC may assign specific work to a task force. The SC will approve the scope of each task force it forms. The SC chair will appoint the task force officers (typically a chair and a vice chair). Each task force will have a finite duration, normally less than one year. The SC will review the task force scope at the end of the expected duration and at each subsequent meeting of the SC until the task force is retired. Action of the SC is required to continue the task force past its defined duration. The SC should consider promoting to a working group any task force that is required to work longer than one year.

Chapter 9: Meetings

Open Meetings

Committee meetings shall be open to all interested parties, subject to any preregistration meeting requirements included in the meeting announcement. Meeting notices shall describe the meeting's purpose and identify a readily available source for further information about the meeting. Only voting members may act on items before the Committee. The Committee secretary shall post meeting notices and agendas on the NERC website contemporaneously with distribution to Committee members. The Committee secretary shall publicly post final minutes of Committee meetings on the NERC website within five business days of Committee approval.

General Requirements

The Committee shall hold meetings as needed and may use conference calls or e-mail to conduct its business.

Notice

The Committee secretary shall announce regularly scheduled meetings with a written notice (letter, facsimile, or e-mail) to all Committee members not less than ten nor more than sixty calendar days prior to the meeting date.

Agenda

The secretary shall provide an agenda with a written notice (letter, facsimile, or e-mail) for Committee meetings no less than five business days before a proposed meeting.

- The agenda shall include, as necessary, background material for agenda items requiring a decision or vote. The secretary shall post the agenda on the NERC website the same day it is distributed to Committee members.
- Items not in the agenda that require a vote cannot be added at a meeting without the unanimous consent of the members present. If such a matter arises, it may also be deferred to the next meeting to allow Committee members to consult with their industry segments.

Parliamentary Procedures

In the absence of specific provisions in this Charter, the Committee shall conduct its meetings guided by the most recent edition of *Robert's Rules of Order, Newly Revised*.

Quorum

A quorum requires two-thirds of the Committee voting members.

Voting

Voting may take place during regularly scheduled meetings or through electronic means.

- All Committee actions shall be approved upon receipt of the affirmative vote of a majority of the members present and voting at a meeting with a quorum present, with the exception of revisions to the Standard Processes Manual and the Committee Charter which can be approved only upon receipt of the affirmative vote of two-thirds of the members present and voting at a meeting with a quorum present.
- Each individual member's vote for each action taken shall be included in the minutes of each meeting, unless the vote is unanimous with no abstentions.

Actions without a Meeting

The Committee may act by mail or e-mail ballot without a regularly scheduled meeting. A majority of the members participating in the voting is required to approve any action. A quorum for actions without a meeting is two-thirds of

Committee members. The Committee chair or four members (each from a different industry segment) may initiate the request for an action without a meeting. The secretary shall post a notice on the NERC website and provide Committee members a written notice (letter, facsimile, or e-mail) of the subject matter for action not less than three business days prior to the date on which the vote is to be counted. The secretary shall both distribute a written notice to the Committee (letter, facsimile, or e-mail) of the results of such action within five business days following the vote and post the results on the NERC website. The secretary shall keep a record of all responses (e-mails, facsimiles, etc.) from the Committee members with the Committee minutes.

Waivers

From time to time it may be necessary to develop a new or modified Reliability Standard, definition, Variance, Interpretation, or implementation plan under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn't sufficient time to follow all the steps in the normal Reliability Standards development process. The Standards Committee may waive any of the provisions contained in the Standard Processes Manual for good cause shown, but limited to the circumstances established in Section 16.0 of the Manual. A waiver request may be submitted to the Committee by any entity or individual. Prior to consideration of any waiver request, the Standards Committee must provide five business days' notice to stakeholders. This provision shall not be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

Proxies

A Committee member may designate a proxy. Proxies may attend and vote at Committee meetings provided the absent Committee member notifies in writing (letter, facsimile, or e-mail) the Committee chair, vice chair or secretary along with the reason(s) for the proxy. The member shall name the proxy representative and affiliation in the correspondence. No Committee member can serve as a proxy for another Committee member. The proxy must adhere to the Voting Members' Expectations and Responsibilities as described in Section 6, above.

Agenda Item 15
Standards Committee
December 13, 2023

2024 Standards Committee Executive Committee Nominations

Action
Inform

Background
In accordance with the Standards Committee (SC) Charter Chapter 7, the Standards Committee Executive Committee (SCEC) shall have a SCEC consisting of no less than five or up to seven members, including the SC officers plus three to five segment members elected by the SC. The segment members cannot represent the same industry segments the SC officers previously represented, nor can any two of the segment members be from the same segment. The SCEC will be elected annually at the January SC meeting. The SCEC shall meet when necessary between regularly scheduled SC meetings to conduct SC business.

2024 SC officers will include:

- SC Chair: Todd Bennett, AECI, formerly representing Segment 3
- SC Vice Chair: Troy Brumfiel, formerly representing Segment 1

Those interested in serving on the SCEC should submit their biography via email to the SC chair, vice chair, and secretary by January 3, 2024.

SPSEG Process Improvement Recommendations Work Plan Status Report

Action
Inform

Summary
At its March 22, 2023 the Standards Committee (SC) approved a work plan to implement the Standards Process Stakeholder Engagement Group (SPSEG) recommendations related to the standards development process administration and SC business practices. The individual recommendations were assigned to various resources; the current status is detailed below.

#	Recommendation	Activities	Resources	Status
1	Appoint a single drafting team to address both SAR and standard development phases	• No conforming SPM changes required • Review and update other process documentation to identify and remove any drafting team references which do not conform to the SPM	SCPS	Complete*
2	Provide guidance to drafting teams on the role of the SAR in standards development process	• Incorporate guidance into drafting team reference manual, and other applicable drafting team resources • Incorporate into work of the SCCG SPSEG recommendation review of SAR form	SCPS, NERC staff SC leadership, SCCG	Complete* Complete
3	Implement changes in administration of SARs for projects posted for informal comment as follows: • Clarify that SARs endorsed by the RSTC or other industry stakeholder groups have had some vetting by industry and qualify for informal comment[1] • Clarify that re-acceptance of SARs is not required for SARs posted for informal comment without material changes in response to comments	• Incorporate into proposed revisions of the SPM • Incorporate into SC new member training	NERC staff SC Leadership	Complete Complete

[1] Through the public comment to the revisions to the SPM, the outcome of this recommendation has evolved to clarify in the SPM that the "some vetting by industry" is to be determined by the SC.

4	Implement changes in administration of SARs for projects posted for formal comment as follows: • SC questions regarding technical support should be referred to the RSTC or posted for comment consistent with the SPM • Provide guidance to drafting teams to assess if a project has sufficient stakeholder support, including developing a list of uniform questions to be used during comment periods for that purpose	• Review applicable portions of SPM with the SC and incorporate into new SC member training • Develop uniform questions for comment periods to clearly gauge industry support	SC leadership SCPS, NERC Staff	Complete Complete
5	Revise the SC Charter to incorporate additional recommendations as follows: • Expand the authority of the SCEC to authorize administrative actions (e.g., posting for supplemental drafting team nomination periods and posting for supplemental SARs for projects in active development) • Expand the authority of the SCEC to approve procedural actions relating to supplemental or revised SAR postings during the standard drafting phase, as well as the authority to allow shortened informal comment periods for such SARs • Clarify the roles of the Chair and Vice Chair on the SCEC • Allow for up to 7 members of the SCEC • Clarify actions by the SCEC must be open to the public, documented in meetings, and reported to the full SC at the next regularly scheduled meeting	• Revise SC Charter to incorporate	SCEC, SC	Complete**
6	SCEC should consider changes when developing agendas as follows: • Consider expanded use of the consent agenda • Consider more frequent use of Section 16.0 Waiver to shorten usual process timelines	• Nothing to be codified procedurally • SCEC to discuss and take under advisement	SCEC SCEC, SC	Complete Complete

7	The SC should revise its guidance for drafting teams with respect to: • Drafting team guidance materials to provide drafting teams with flexibility on whether they will develop any implementation guidance during standards • Encourage drafting teams to work closely with NERC Staff on the development of VRFs/VSLs	• Review and update drafting team reference manual and other applicable process documentation • Incorporate guidance into drafting team reference manual, NERC VRF guidelines, NERC VSL guidelines, and applicable other drafting team resources	SCPS SCPS, NERC Staff	Complete* Complete*

* Pending SC Action at January 2024 Meeting
**Pending SC Action at December 13, 2023 Meeting

NERC Legal and Regulatory Update
November 1, 2023 – November 30, 2023

NERC FILINGS TO FERC SUBMITTED SINCE LAST SC UPDATE

FERC Docket No.	Filing Description	FERC Submittal Date
RD23-5-000	Amended Petition for Approval of Proposed Reliability Standard PRC-023-6 As directed by the October 10, 2023 letter order requesting additional information, NERC submitted a petition for approval of proposed Reliability Standard PRC-023-6.	11/3/2023
RD22-4-001	Inverter Based Resources Work Plan Progress Update NERC submitted a progress update on its Inverter Based Resources Work Plan as directed by FERC in its November 17, 2022 Order.	11/14/2023

FERC ISSUANCES SINCE LAST SC UPDATE

FERC Docket No.	Issuance Description	FERC Issuance Date
RD23-4-000	Order Approving Standards ROP Revisions FERC issued an Order approving revisions to the NERC Rules of Procedure (ROP) regarding Reliability Standards Development. The order also directs a compliance filing within 18 months.	11/23/2023
RD23-6-000	Order Approving Reliability Standards IRO-010-5 and TOP-003-6.1 FERC issued a letter order approving Reliability Standards IRO-010-5 and TOP-003-6.1.	11/2/2023
RM19-17-001	Order No. 902- Final Rule to Retire the MOD A Reliability Standards and Requirements FERC issued a Final Rule approving NERC's request to retire the MOD A Reliability Standards and requirements.	10/26/2023

ANTICIPATED UPCOMING FILINGS

FERC Docket No.	Filing Description	Anticipated Filing Date
RM05-17-000; RM05-25-000; RM06-16-000	2024-2026 Reliability Standards Development Plan (RSDP) annual filing	12/15/2023
TBD	Petition for Approval of VAR-501-WECC-4	12/15/2023
RD20-2-000	CIP Standard Drafting Team Schedule Update Informational Filing	12/15/2023
TBD	WECC BAL Directive (Order No. 876)	12/2023
TBD	Petition for approval of CIP-012	1/12/2024