NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

September 20, 2023 | 10:00 a.m.—3:00 p.m. Eastern

NERC – Washington Office
1401 H Street N.W., Suite 410
Washington, DC 20005

SC Meeting in Capital Room (414)

Dial-in: 1-415-655-0002 | Access Code: 2303 940 8105 | Meeting Password: 092023
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 September 20, 2023 Agenda - Approve - *Amy Casuscelli* (1 minute)**
2. **Consent Agenda - Approve - *Amy Casuscelli* (5 minutes)**
   a. August 23, 2023 Standards Committee Meeting Minutes* - **Approve**
   b. Drafting Team Nominee Selection Criteria - **Approve**
      i. Drafting Team Nominee Selection Criteria*
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)
4. **Chair and Vice Chair Elections - Elect - *Alison Oswald (5 minutes)***
5. **2024-2025 Term Elections - Inform - *Alison Oswald (5 minutes)***
6. **CIP-013-2 Supply Chain Risk Management Standard Authorization Request - Accept/Authorize/Authorize - *Jamie Calderon (10 minutes)***
   a. CIP-013-2 Supply Chain Risk Management Standard Authorization Request*
7. **Project 2021-03 CIP-002 - Authorize - *Latrice Harkness (10 minutes)***
   a. CIP-002-Y*

b. Implementation Plan*

8. **Standards Process Stakeholder Engagement Group Process Improvement Recommendations - Inform - *Amy Casuscelli (10 minutes)***
9. **Project Prioritization - Inform - *Latrice Harkness (10 minutes)***
10. **Project Updates**
    a. 2016-02 Modifications to CIP Standards - *Jay Cribb and Matt Hyatt* (15 minutes)
    b. 2017 Modifications to BAL-003 Phase II - *David Lemmons* (15 minutes)
    c. 2019-04 Modifications to PRC-005-6 - (15 minutes)
    d. 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination - *Matt Harward* (15 minutes)
11. **Subcommittee Updates**
    a. Project Management and Oversight Subcommittee (PMOS) - *Mike Brytowski* (10 minutes)
    b. Standards Committee Process Subcommittee (SCPS) - *Matt Harward* (10 minutes)
    c. Standing Committees Coordinating Group (SCCG) - *Todd Bennett* (10 minutes)
    d. Reliability and Security Technical Committee (RSTC) - *Amy Casuscelli* (10 minutes)
    e. NERC Board of Trustees - *George Hawkins* (10 minutes)
12. **Legal Update and Upcoming Standards Filings - Review - *Sarah Crawford* (5 minutes)**
13. **Informational Items - Enclosed**
    a. Standards Committee Expectations*
    b. 2023 SC Meeting Schedule
    c. 2023 Standards Committee Roster
    d. Highlights of Parliamentary Procedure*
14. **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

A. Casuscelli, chair, called to order the meeting of the Standards Committee (SC) on August 23, 2023, at 1:02 p.m. Eastern. A. Oswald called roll and determined the meeting had a quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement
The SC secretary 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.

Review August 23, 2023 Agenda (agenda item 1)
The SC approved the August 23, 2023 meeting agenda.

Consent Agenda (agenda item 2)
The SC approved the July 19, 2023 SC Meeting Minutes. The SC was informed about Project 2023-04 Modifications to CIP-003 SC Action without a Meeting.

Projects Under Development (agenda item 3)
C. Yeung reviewed the Project Tracking Spreadsheet. L. Harkness reviewed the Project Posting Schedule.

Project Management Posting Coordination (agenda item 4)
M. Brytowski provided an overview of the Project Management Oversight Subcommittee (PMOS) posting coordination. C. Yeung provided insight into how liaisons could work with developers and drafting team (DT) leadership to coordinate schedules. S. Kim shared that Standard Development is looking to host a webinar that details the prioritization of projects and the risk registry update. Discussion will continue to the next SC meeting.

Legal Update and Upcoming Standards Filings (agenda item 9)
L. Perotti provided an update.

Errata to Reliability Standard TOP-003-6 (agenda item 6)
L. Harkness provided an overview of the errata changes. V. O'Leary motioned to accept the errata changes to TOP-003-6 to remove the word "using" from Requirement R5 and correct the grammar of the word "methods" in Requirement R2 Part 2.5.5.

The SC approved the motion with no objections or abstentions.

Project 2023-03 Internal Network Security Monitoring (agenda item 5)
J. Calderon provided an overview of the project background and standard authorization request (SAR). S. Rueckert made a motion to accept the revised Project 2023-03 Internal Network Security Monitoring Standard Authorization Request (SAR), authorize drafting of Reliability Standard(s) identified in the SAR, and approve a waiver of provisions of the Standard Processes Manual for Project 2023-03 Internal Network Security Monitoring (INSM) due to regulatory deadlines, as follows:

- Initial formal comment and ballot period reduced from 45 days to as few as 30 calendar days, with ballot pools formed in the first 20 days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last five days of the comment period (Sections 4.9, 4.10);
- Additional formal comment and ballot period(s) reduced from 45 days to as few as 20 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period (Sections 4.9, 4.10).
- Final ballot reduced from 10 days to as few as five calendar days (Section 4.13)

The SC approved the motion with no objections or abstentions.

Project 2021-08 Modifications to FAC-008 (agenda item 7)
J. Calderon provided an overview of the project background. V. O'Leary asked if the additional requirement nine aligned with the SAR's scope. B. Wu shared that requirement nine complements requirement 6, which requirement 9 focuses on maintaining data to keep requirement six enforceable. V. O'Leary made a motion to authorize initial posting of the proposed Reliability Standard FAC-008-6 and the associated Implementation Plan for a 45-day formal comment period, with ballot pools formed in the first 30 days and parallel initial ballots and non-binding polls on the VRFs and VSLs, conducted during the last 10 days of the comment period.

The SC approved the motion with no objections or abstentions.

Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination (agenda item 8)
L. Harkness provided an overview of the project's background. S. Rueckert inquired when the SDT would have to respond to comments from the last formal comment period. A. Oswald mentioned that the SDT would have enough time to respond to comments. S. Rueckert made a motion to 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 20 days, with the 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)

The SC approved the motion with no abstentions. William Chambliss, Kent Feliks, and Terri Pyle opposed.

R. Blohm asked about the classifications of NERC membership sectors and, specifically, inquired about the ”associate” category and how it is defined. L. Perotti explained how the NERC membership sectors differ from the registered body segments and provided a brief overview.

Adjournment

The meeting adjourned at 2:29 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 1-2021-22	Troy Brumfield* Regulatory Compliance Manager	American Transmission Company		X
Segment 2-2022-23	Jamie Johnson Infrastructure Compliance Manager	California ISO		N
Segment 2-2021-22	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 3-2021-22	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 4-2021-22	Patti Metro Senior Grid Operations & Reliability Director	National Rural Electric Cooperative Associate	Alice Wright	X
Segment 5-2022-23	Terri Pyle Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric		X
Segment 5-2021-22	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 6-2021-22	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 7-2021-22	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	Independent		X
Segment 9-2022-23	Sarosh Muncherji[1] Cyber Security Specialist	British Columbia Utilities Commission		X
Segment 9-2021-22	William Chambliss General Counsel	Virginia State Corporation Commission		X
Segment 10-2022-23	Tony Purgar Senior Manager, Operational Analysis & Awareness	ReliabilityFirst		X
Segment 10-2021-22	Steven Rueckert Director of Standards	WECC		X

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

Revised Standards Committee Guideline: Drafting Team Nominee Selection Criteria

Action
Approve

Background
On May 16, 2023, the Standards Committee Process Subcommittee (SCPS) started a subgroup to review the Drafting Team Nominee Selection Criteria and the Drafting Team Reference Manual. The subgroup conducted its first of six meetings on June 13, 2023. The subgroup proposed revisions for the Drafting Team Nominee Selection Criteria and determined no modifications were necessary for the Drafting Team Reference Manual.

On August 14, 2023, the SCPS conducted an email vote to approve the Drafting Team Nominee Selection Criteria resource document changes. The vote passed with nine out of the 12 members voting and receiving nine out of nine in favor of the edits.

Summary
The subgroup made minor edits to the Drafting Team Nominee Selection Criteria document to ensure clarity, update, and remove redundant language.

The team also reviewed the Drafting Team reference manual and found no changes or edits were necessary since the last review.

Additional Information
More information is available on the project page.

Standards Committee Guideline

Drafting Team Nominee Selection Criteria

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

Purpose: To provide eligibility criteria for appointment to a Drafting Team.

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

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

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

The SC will follow the *Standard Processes Manual* when forming a DT.

In most cases, when a DT is to be appointed, NERC staff will post a notice on the NERC website, requesting that interested parties complete and submit a DT nomination form. The Director of Standards Development will review the list of candidates and provide a recommended slate of nominees to the SC, including each individual's letter(s) of recommendation if provided with the nomination materials. The recommended slate of nominees will include a recommendation for a chair and a vice chair.

The size of the DT should depend in large part on the scope and complexity of the work that will be assigned to it. Simple, non-controversial changes to a single standard benefit from the efficiencies gained through consideration by a smaller DT (such as five to seven members). Complex projects that entail changes to multiple standards or development of a controversial, complicated new standard could benefit from a larger team with the capacity to work in subteams, broad subject-matter diversity and depth of knowledge, and the necessary industry outreach. If a project is anticipated to require a greater time

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

commitment, the number of DT members needs to be sufficient to provide continuity as competing demands on members' time fluctuate.

The SC has the responsibility and authority to make the final determination on appointment to DTs and considers each candidate's technical experience in the specific issue being addressed as well as the ability to work effectively towards consensus in a group situation . In making appointments, the SC considers the following qualifications:

i. Verifiable requisite subject matter expertise;
ii. Representation from as many NERC Regions as possible, with particular consideration given to including each Region with an identified Regional variance. This may consist of any or all of the following;
    a. Technical knowledge of regional criteria (Regional staff and/or NERC staff may verify regional participation, references provided by the candidate in the nomination form, or verify knowledge by other means.)
    b. Operational experience in the region
    c. Asset ownership in the region
iii. Representation from each Interconnection;
iv. Representation from Canada and the United States;
v. Representation from each of the functional entities expected to have compliance obligations in the proposed standard;
vi. Representation from as many impacted industry segments as possible;
vii. Prior standard development experience and the number of drafting teams the candidate already represents; and
viii. Regulatory, legal and/or compliance expertise.

If more than one candidate provides a similar set of qualifications and diversity, preference may be given to appointing the candidate who possesses any of the following qualifications:

a. Is an employee or agent of a NERC registered entity;
b. Has experience, or is familiar with, NERC standards drafting (though not mandatory so as not to limit participation of new members);
c. Has proven experience working in a team environment (NERC staff may verify past experience and active participation/performance in NERC or Regional committees, working groups or task forces).

If the initial pool of nominations does not provide the mix of candidates needed to ensure that there is sufficient technical expertise with diverse views to represent the industry's viewpoints, additional nominations may be solicited.

If there is a vacancy on a DT, the SC shall consider the following, in addition to the previous stated qualifications, when determining whether to appoint DT replacements:

i. Whether there is a candidate who has the requisite subject matter expertise and has been an active observer, already receiving drafting team material.

ii. Whether a candidate has similar expertise as the individual being replaced.

iii. Whether there are qualified candidates who submitted a formal application for a position on the team but were not appointed.

iv. Whether the project schedule includes sufficient work to warrant replacing the drafting team member.

The SC may direct staff to post a request for additional nominations, opening the nomination process to all interested parties.

Expectations: All Drafting Team members are required to adhere to the *NERC Participant Conduct Policy* and *Drafting Team Reference Manual*.

Version History

Version	Date	Owner	Change Tracking
1	March 14, 2018	NERC Standards Committee	N/A
2	March 18, 2020	NERC Standards Committee	Minor edits and removal of redundant text
3	September 07, 2021	NERC Standards Committee	Incorporate drafting team selection guidance language from *Standards Drafting Team Scope*
4	July 06, 2023	NERC Standards Committee Process Subcommittee	Minor edits of language and removal of redundant text.

Standards Committee Guideline

Drafting Team Nominee Selection Criteria

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

Purpose: To provide eligibility criteria for appointment to a Drafting Team.

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

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

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

The SC will follow the *Standard Processes Manual* when forming a DT.

In most cases, when a DT is to be appointed, NERC staff will post a notice on the NERC website, requesting that interested parties complete and submit a DT nomination form. The Director of Standards Development will review the list of candidates and provide a recommended slate of nominees to the SC, including each individual's letter(s) of recommendation if provided with the nomination materials. The recommended slate of nominees will include a recommendation for a chair and a vice chair.

The size of the DT should depend in large part on the scope and complexity of the work that will be assigned to it. Simple, non-controversial changes to a single standard benefit from the efficiencies gained through consideration by a smaller DT (such as five to seven members). Complex projects that entail changes to multiple standards or development of a controversial, complicated new standard could benefit from a larger team with the capacity to work in subteams, broad subject-matter diversity and depth of knowledge, and the necessary industry outreach. If a project is anticipated to require a greater time

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

commitment, the number of DT members needs to be sufficient to provide continuity as competing demands on members' time fluctuate.

The SC has the responsibility and authority to make the final determination on appointment to DTs and considers each candidate's technical experience in the specific issue being addressed as well as the ability to work effectively towards consensus in a group situation. In making appointments, the SC considers the following qualifications:

i. Verifiable requisite subject matter expertise;
ii. Representation from as many NERC Regions as possible, with particular consideration given to including each Region with an identified Regional variance. This may consist of any or all of the following;
    a. Technical knowledge of regional criteria (Regional staff and/or NERC staff may verify regional participation, references provided by the candidate in the nomination form, or verify knowledge by other means.)
    b. Operational experience in the region
    c. Asset ownership in the region
iii. Representation from each Interconnection;
~~iii.~~iv. Representation from Canada and the United States;
~~iv.~~v. Representation from each of the functional entities expected to have compliance obligations in the proposed standard;
~~v.~~i. ~~Representation from Canada and the United States;~~
vi. Representation from as many impacted industry segments as possible;
vii. Prior standard development experience and the number of drafting teams the candidate already represents; and
viii. Regulatory, legal and/or compliance expertise.

If more than one candidate provides a similar set of qualifications and diversity, preference may be given to appointing the candidate who possesses any of the following qualifications:

a. Is an employee or agent of a NERC registered entity;
b. Has experience, or is familiar with, NERC standards drafting (though not mandatory so as not to limit participation of new members);
c. Has proven experience working in a team environment (NERC staff may verify past experience and active participation/performance in NERC or Regional committees, working groups or task forces).

If the initial pool of nominations does not provide the mix of candidates needed to ensure that there is sufficient technical expertise with diverse views to represent the industry's viewpoints, additional nominations may be solicited.

If there is a vacancy on a DT, the SC shall consider the following, in addition to the previous stated qualifications, when determining whether to appoint DT replacements:

i. Whether there is a candidate who has the requisite subject matter expertise and has been an active observer, already receiving drafting team material.

ii. Whether a candidate has similar expertise as the individual being replaced.

iii. Whether there are qualified candidates who submitted a formal application for a position on the team but were not appointed.

iv. Whether the project schedule includes sufficient work to warrant replacing the drafting team member.

The SC may direct staff to post a request for additional nominations, opening the nomination process to all interested parties.

Expectations: All Drafting Team members are required to adhere to the *NERC Participant Conduct Policy* and *Drafting Team Reference Manual*.

Version History

Version	Date	Owner	Change Tracking
1	March 14, 2018	NERC Standards Committee	N/A
2	March 18, 2020	NERC Standards Committee	Minor edits and removal of redundant text
3	September 07, 2021	NERC Standards Committee	Incorporate drafting team selection guidance language from *Standards Drafting Team Scope*
4	July 06, 2023	NERC Standards Committee Process Subcommittee	Minor edits of language and removal of redundant text.

Standards Committee Actions - 3 Month Outlook

September 2023

Authorize Initial Posting

2021-03 CIP-002 (TOCC)

October 2023

Accept Revised SAR

2023-02 Performance of IBRs

Appoint Drafting Team

2023-06 CIP-014 Risk Assessment Refinement

2023-07 Modifications to TPL-001-5.1 Transmission System Planning Performance Requirements for Extreme Weather

Authorize Initial Posting

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

2020-06 Verifications of Model and Data for Generators

2023-03 Internal Network Security Monitoring (INSM)

2023-04 CIP-003 LICRT

November 2023

Accept Revised SAR

2023-07 Modifications to TPL-001-5.1 Transmission System Planning Performance Requirements for Extreme Weather

Authorize Initial Posting

2022-03 Energy Assurance with Energy-Constrained Resources

December 2023

Accept Revised SAR

2023-06 CIP-014 Risk Assessment Refinement

Standards Committee Chair and Vice Chair Election

Action

Elect the chair and vice chair of the Standards Committee (SC) for a two-year term starting January 1, 2024 - December 31, 2025.

Background

At the September 20, 2023 SC meeting, elections for the chair and vice chair will be conducted immediately after the consent agenda is completed. The elections shall be accomplished as follows:

a. The nominating committee will ask if there are any nominations from the floor. If there is a nomination from the floor, the nominee shall be provided five minutes to present his or her qualifications to the SC orally.

b. After (a) is completed, the Secretary of the SC shall distribute electronic election ballots for both chair and vice chair. The members shall indicate their selection on the ballot and return the ballot to the Secretary. The current chair and vice chair have the right to vote in both elections for chair and vice chair.

The following individuals were nominated for the chair and vice chair positions, respectively:

Todd Bennett, Formally Segment 3, Nominated for Chair

Mr. Bennett's involvement in the utility sector began in 2001, NERC compliance initiatives have been a focus of his since 2009, which have been supported through participation as a NERC SC member since 2018. As an active participant in multiple industry peer groups, Mr. Bennett has demonstrated leadership through roles as chair of the SERC Registered Entity Forum, co-chair of the NERC Functional Model Task Force, chair of the NERC Standing Committees Coordinating Group, and vice-chair of the NERC SC. Mr. Bennett's current duties at AECI include management of the AECI NERC compliance program, internal NERC standards compliance monitoring, NERC standards development input, and implementation of an AECI board approved internal audit work plan.

Mr. Bennett's industry background includes seven years at Sho-Me Power Electric Cooperative as an engineer and 15 years at AECI working on NERC compliance through multiple leadership roles. Areas of focus while at AECI include operations, planning, and critical infrastructure protection issues. AECI is registered as a Jointly Registered Organization (JRO) for the following functions: BA, DP, GO, GOP, PC, RP, TO, TOP, TP, and TSP; resolving operational issues based on these functional registrations has made Mr. Bennett deeply aware of the current challenges that NERC and industry stakeholders are facing.

Mr. Bennett obtained a BS in Engineering from the University of Missouri and an MS of Engineering Management from the Missouri Institute of Science & Technology. Mr. Bennett is a registered Professional Engineer (PE) in the state of Missouri and maintains Certified Internal Auditor (CIA) and Certification in Risk Management Assurance (CRMA) certifications through the Institute of Internal Auditors.

Charles Yeung, Segment 2, Nominated for Chair
As Executive Director of Interregional Affairs at Southwest Power Pool (SPP) for 19 years, Charles has led SPP's participation in the NERC standards process providing comments on NERC standards projects and matters related to the reliability of the North American Electric grid since the creation of the ERO. Charles is currently serving as the Vice Chair of the Project Management Oversight Subcommittee and has been in both Chair and Vice Chair roles since 2016. His first term on the NERC SC was in 2013, when he supported the formation of PMOS and the development of the Project Tracking Spreadsheet.

Charles is an Electrical Engineer and also holds a Master of Business Administration. He has worked in the power utility industry since 1988 with experience in transmission system protection, short circuit modeling, and analysis, as well as state and FERC level open access regulatory policy development.

Charles is also a member of other NERC groups, such as the Electric Gas Working Group, and has served on the Reliability Issues Steering Committee. Prior to Order 693 and Version 0 NERC standards, Charles developed the SPP Regional Entity Standards Development Process to satisfy the SPP Regional Entity Delegation Agreement.

Troy Brumfield, Segment 1, Nominated for Vice Chair
Troy Brumfield is an employee at American Transmission Company, LLC (ATC). His current position is Manager Reliability Standards Compliance. In this role, Mr. Brumfield is responsible for leading the overall development and directing the activities and execution of ATC's regulatory strategy; (2) monitoring ATC's regulatory environment; (3) representing ATC at industry committees and trade organization meetings; and (4) working with ATC legal staff to develop regulatory strategies and resolve compliance and enforcement related issues.

Mr. Brumfield is a current member of the NERC SC and actively participates in the subcommittees that report to the SC. He is currently serving as the Vice-Chair of the Standards Committee Process Subcommittee (SCPS) and serves as a member of the Standards Committee Executive Committee (SCEC).

Mr. Brumfield is also a member of the Midwest Reliability Organization's (MRO) Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC). The CMEPAC provides advice and counsel to MRO's Board of Directors, staff, members, and registered entities on topics like the development, retirement, and application of NERC Reliability Standards, risk assessment, compliance monitoring, and the enforcement of applicable standards.

He has been a chair and contributing member to several NERC Standards Drafting Teams and NERC Initiative Teams.

- NERC project 2017-07 Standards Alignment with Registration
- Guidelines and Technical Basis (GTB) Review Team
- Standards Efficiency review- Phase 1 Team (sub-team chair)
- Member- NERC Compliance and Certification Committee- ERO Monitoring Subcommittee.

- Observer and Active participant-2018-03 Standards Efficiency Review Retirements project
- Member-MRO NERC Standards Review Forum

Prior to joining ATC, Mr. Brumfield was employed at Wisconsin Energy Corporation (WEC). While at WEC, Mr. Brumfield held various leadership roles in the Operations and Engineering-Major Projects work group and the Operations Support group, where he was responsible for managing regulatory obligations, standards development, compliance, and asset management. During his time at WEC, Mr. Brumfield served as Chair of several generation and distribution regional committees and councils that were tasked with promoting and strengthening governmental and industry partnerships. Mr. Brumfield utilized these committees and councils as a forum to facilitate discussions related to standards interpretation and standards execution by utility and governmental employees focused on the reliable design, construction, operation, and maintenance of electric and gas facilities.

Mr. Brumfield earned a Bachelor of Applied Science in Electronics Engineering Technology. He also earned a Master of Science in Engineering Management from the Milwaukee School of Engineering University.

Please use this link or QR code below for the Officer Election. This poll will not be live until announced in the Standards Committee meeting.

Standards Committee 2024-2025 Term Elections

Action
Inform

Background
Per the Rules of Procedure Appendix 3b, "Standards Committee membership shall be for a term of two years, with members' terms staggered such that half of the member positions (one per Segment) are refilled each year by Segment election. Prior to the end of each term, nominations will be received, and an election will be held in accordance with this procedure, or a qualified Segment procedure, to elect Standards Committee representatives for the next term. There is no limit on the number of two-year terms that a member of the Standards Committee may serve, although the setting of limits in the future is not precluded." Additionally, no two persons employed by the same corporation or organization or an affiliate may serve concurrently as Committee members. (Standards Committee Charter, Chapter 4)

Term elections for the 2024-2025 term will begin in October 2023 and follow the schedule below.

- October 3 – 23, 2023: Nominations accepted from industry
- November 1 – 13, 2023: Election held
- November 16, 2023: Election results announced

Included is a list of Standards Committee members whose terms are ending and are up for reelection

Segment and Terms	Representative	Organization
Segment 1-2022-23	Michael Jones Manager, Reliability Standards & Policy	National Grid
Segment 2-2022-23	Jamie Johnson Infrastructure Compliance Manager	California ISO
Segment 3-2022-23	Kent Feliks Manager NERC Reliability Assurance – Strategic Initiatives	American Electric Power Company, Inc.
Segment 4-2022-23	Marty Hostler Reliability Compliance Manager	Northern California Power Agency
Segment 5-2022-23	Terri Pyle Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric
Segment 6-2022-23	Sarah Snow* Manager of Reliability Compliance	Cooperative Energy

Segment 7-2022-23	Kristine Martz Industry Specialist, Power & Utilities	Amazon Web Services
Segment 8-2022-23	Robert Blohm[1] Managing Director	Keen Resources Ltd.
Segment 9-2022-23	Sarosh Muncherji[1] Cyber Security Specialist	British Columbia Utilities Commission
Segment 10-2022-23	Tony Purgar Senior Manager, Operational Analysis & Awareness	ReliabilityFirst

[1] Serving as Canadian Representative

*Denotes SC Executive Committee Member

CIP-013-2 Supply Chain Risk Management

Action

- Accept the CIP-013-2 – Supply Chain Risk Management[1] Standard Authorization Request (SAR) submitted by the NERC critical infrastructure protection technical and compliance staff;
- Authorize posting of the SAR for a 30-day formal comment period; and
- Authorize solicitation of the SAR drafting team (DT) members.

Background

This project would address the current implementation of CIP-013, which has been wide-ranging and variable, potentially leading to incomplete or inaccurate supply chain risk evaluations. This project would revise CIP-013 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity. Additionally, it would provide triggers on when the supply chain risk assessment(s) must be performed (i.e., planning for procurement, procurement, and installation) and require a response to risks identified.

Summary

NERC staff recommends that the Standards Committee accept the CIP-013-2 SAR, authorize its posting for a 30-day formal comment period, and authorize the solicitation of DT members.

[1] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.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:	CIP-013-2 Supply Chain Risk Management SAR		
Date Submitted:	September 18, 2023		
SAR Requester			
Name:	Michaelson Buchanan		
Organization:	NERC		
Telephone:	470.725.5268	Email:	michaelson.buchanan@nerc.net

SAR Type (Check as many as apply)

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

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

- ☒ Regulatory Initiation
- ☐ Emerging Risk (Reliability Issues Steering Committee) Identified
- ☐ Reliability Standard Development Plan
- ☐ NERC Standing Committee Identified
- ☐ Enhanced Periodic Review Initiated
- ☐ Industry Stakeholder Identified

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

The language in CIP-013-2 Requirement R1 lacks specificity to properly identify, assess, and respond to supply chain security risks. Specifically, Requirement R1 Part 1.1 does not indicate how to perform risk identification and assess vendor risks effectively. Additionally, CIP-013-2 does not contain sufficient triggers requiring activating an entity's supply chain risk management plan.

Industry implementation is wide ranging and variable across the ERO Enterprise. The implemented Industry supply chain risk processes are ambiguous and generally lack rigor for validating the completeness and accuracy of the data, assessing the risks, considering the vendor's mitigation activities, and documenting and tracking residual risks. This also leads to inconsistent information collected from vendors.

The lack of specificity for correctly identifying and assessing supply chain security risks may lead to incomplete or inaccurate risk evaluations. This may lead to supply chain risk likelihood and/or impact ratings that are not truly reflective of the actual risk posed to the entity.

Requested information
There is a lack of activation triggers to perform an entity's supply chain risk management program. The ambiguous language of Requirement R2's "Note" and the potential for a sizeable time delay between the actual procurement of equipment and the installation of the procured equipment. This delay could render the risk assessment outdated and potentially inaccurate during installation. An updated or revised risk assessment would ensure that all current and relevant risks are identified, assessed, and addressed. A requirement to update or re-perform a risk assessment for equipment or software before installation is necessary, as well as a time limit between the assessment and installation. There is a lack of tracking or responding to the risks identified through an entity's supply chain risk assessment. Requirement R1 Part 1.1 requires entities to "identify and assess," but the Standard does not require an entity to take any actions (i.e., respond) to any identified risks through the risk assessment. This includes accepting risks if they fall within a certain threshold. If accepted risks increase over time to a level above the entity's threshold, the entity may not be aware of the change due to the lack of tracking said risks. The majority, if not all, risk management frameworks hold fast to three pillars: 1. Identify, 2. Assess, and 3. Respond. Industry has many options to respond to risks, including mitigation, acceptance, transfer, and/or avoidance. Regardless of the option chosen, a response includes documenting and tracking the risk(s).
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This project would revise CIP-013-2 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity. Additionally, it would provide triggers on when the supply chain risk assessment(s) must be performed (i.e., planning for procurement, procurement, and installation) and require a response to risks identified.
Project Scope (Define the parameters of the proposed project):
This project will make revisions to CIP-013-2 to require complete and accurate assessments of supply chain risks. Provide triggers of when activation of the supply chain risk assessment(s) must be performed and tracking and responding to all risks identified.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide (1) a technical justification[1] that 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):
Revise CIP-013-2 to: • Require entities to create specific triggers to activate the supply chain risk assessment(s).

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

Requested information
• Include the performance of supply chain risk assessment(s) during the planning for procurement, procurement, installation of procured equipment/software/services, and post procurement assessment. • Include steps to validate the completeness and accuracy of the data, assess the risks, consider the vendor's mitigation activities, and document and track any residual risks. • Track and respond to all risks identified. • Re-assessment of standing contract risks on a set timeframe. • Re-assessment of time delay installation beyond a set timeframe.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The Cost impact of implementing the proposed Standard depends on the method(s) by which a Responsible Entity chooses to meet any additional Requirements. However, a question will be asked during the comment period to ensure cost aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
No unique characteristics of BES facilities that may be impacted are known at this time.
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):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide recommendations or findings from the consensus building activity.
SAR was developed in cooperation with and reviewed by voting members of the ERO CIP Compliance Task Force.
Are there any related standards or SARs that should be assessed for impact due to this proposed project? If so, which standard(s) or project number(s)?
None at this time.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the other options.

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

Requested information
None at this time.

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 operating 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.
☒	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 from 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

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 2021-03 CIP-002

Action

Authorize initial posting of proposed Reliability Standard CIP-002-Y and the associated Implementation Plan for a 45-day formal comment period, with ballot pools formed in the first 30 days and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period.

Background

Project 2021-03 currently has five assigned Standard Authorization Requests (SARs). The proposed standard revisions are based on the Project 2016-02 SAR, which seeks to modify Reliability Standard CIP-002 to address the categorization of specific Transmission Owner Control Centers (TOCC) performing Transmission Operator (TOP) functions as medium impact based on an aggregate weighted value of their BES Transmission Lines in Criterion 2.12.

On May 14, 2020, the NERC Board of Trustees (Board) adopted the proposed Reliability Standard CIP-002-6. The proposed standard revised Criterion 2.12 to categorize certain TOCCs performing Transmission Operator functions as medium impact based on an aggregate weighted value of their Bulk Electric System (BES) Transmission Lines. The Project 2016-02 SAR was accepted by the Standards Committee (SC) on July 20, 2016, which includes the scope for addressing the TOCC obligations.

On June 12, 2020, NERC staff filed with the Federal Energy Regulatory Commission (FERC) a petition to approve proposed CIP-002-6. On June 23, 2020, the proposed standard was filed with the applicable regulatory authorities in Canada.

At its February 4, 2021 meeting, the Board withdrew the proposed Reliability Standard CIP-002-6. In addition, the Board issued a resolution stating "that NERC staff, working with stakeholders, is directed to promptly conduct further study of the need to readdress the applicability of the CIP Reliability Standards to such Control Centers[1] to safeguard reliability, for the purpose of recommending further action to the Board." On February 5, 2021, NERC filed a notice of withdrawal for CIP-002-6 with FERC.

At its March 17, 2021 meeting, the SC authorized solicitation for a Standard Drafting Team (SDT) to conduct a field test and assigned a portion of the Project 2016-02 SAR related to TOCC to the SDT. 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.

[1] In this context, Control Centers refers to those owned by Transmission Owners performing the functional obligations of a Transmission Operator.

From February 2023 – August 31, 2023, the SDT conducted several meetings and a 30-day informal comment period to make revisions to the standard language, associated Implementation Plan, and VRFs and VSLs.

Summary

The Quality Review (QR) for this posting was performed from August 18 – August 25, 2023. The QR team members from NERC were Lauren Perotti and Marisa Hecht. The SDT also reached out to the industry. The QR members from the industry included Todd Bennett (AECI) and Jay Cribb (SoCo).

The SDT reviewed all QR comments and revised the proposed Reliability Standard and Implementation Plan where appropriate.

NERC staff recommends that the SC authorize posting of the proposed Reliability Standard CIP-002-Y and associated Implementation Plan for initial formal comment and ballot.

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved 2016-02 TOCC Standard Authorization Request (SAR) for posting	March 6, 2016
SAR posted for 2016-02 TOCC comment	March 23 – April 21, 2016
SC Accepted the 2016-02 TOCC SAR	July 20, 2016
45-day formal comment period with ballot	September – November 2023

Anticipated Actions	Date
Final Ballot TOCC	December 2023
Board adoption	December 2023

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):

Control Center - One or more rooms where a responsible entity hosts operating personnel to monitor and control the Bulk Electric System (BES) in real-time, as described below, including any spaces that house the Cyber Assets used by operating personnel to monitor and control the BES in real-time. Cyber Assets used by operating personnel to monitor and control the BES in real-time are generally housed in a centralized location and exclude field assets such as remote terminal units.

1) Operating personnel who perform the Real-time reliability-related tasks of a Reliability Coordinator;

2) Operating personnel who perform the Real-time reliability-related tasks of a Balancing Authority;

3) Operating personnel who perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations;

4) Operating personnel of a Transmission Owner who have the capability to electronically control Transmission Facilities at two or more locations in real-time; or

5) Operating personnel of a Generator Operator who have the capability to electronically control generation Facilities at two or more locations in real-time.

A. Introduction

1. Title: Cyber Security — Bulk Electric System (BES) Cyber System Categorization

2. Number: CIP-002-Y

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-Y:

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.

5. Effective Dates: See "Project 2021-03 CIP-002 Transmission Owners Control Centers Implementation Plan"

B. Requirements and Measures

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

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. RAS that support the reliable operation of the BES; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

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

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

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

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

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

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

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

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its

parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each 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.

2. Table of Compliance Elements

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

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-Y - Attachment 1

Impact Rating Criteria

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

1. High Impact Rating (H)

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

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

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

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

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

2. Medium Impact Rating (M)

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

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

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

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

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

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

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

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

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

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

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

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

Each BES Cyber System, not included in Section 1 above, used by and located at any of the following:

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

2.12. Each Control Center or backup Control Center, operated by a Transmission Operator or owned by a Transmission Owner, that is not already included in High Impact Rating (H) above, with an "aggregate weighted value" exceeding 6000 according to the table below and subject to the listed exclusion. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per characteristic" shown in the table for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line
<100 kV	100
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

Exclusion:

BES Transmission Lines monitored and controlled by the Control Center or backup Control Center may be excluded from the "aggregate weighted value" calculation if they are part of a local system that is operated at less than 300kV, where the net export from the local system does not exceed 75 MW during non-Energy Emergency Alert (EEA) conditions. The net export is based on the hourly integrated values for the most recent 12-month period.

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

3. Low Impact Rating (L)

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

3.5. RAS that support the reliable operation of the BES.

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
Y	TBD		

Standard Development Timeline

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

Description of Current Draft

This is the initial draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved 2016-02 TOCC Standard Authorization Request (SAR) for posting	March 6, 2016
SAR posted for 2016-02 TOCC comment	March 23 – April 21, 2016
SC Accepted the 2016-02 TOCC SAR	July 20, 2016
45-day formal comment period with ballot	September – November 2023

Anticipated Actions	Date
Final Ballot TOCC	December 2023
Board adoption	December 2023

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):

Control Center - One or more ~~facilities~~ rooms where a responsible entity hosts ~~hosting~~ operating personnel ~~that~~ to monitor and control the Bulk Electric System (BES) in real-time, as described below, ~~to perform the reliability tasks,~~ including any spaces that house the Cyber Assets used by operating personnel to monitor and control the BES in real-time. Cyber Assets used by operating personnel to monitor and control the BES in real-time are generally housed in a centralized location and exclude field assets such as remote terminal units.~~their associated data centers, of:~~

1) Operating personnel who perform the Real-time reliability-related tasks of a Reliability Coordinator;~~,~~

2) Operating personnel who perform the Real-time reliability-related tasks of a Balancing Authority;~~,~~

3) Operating personnel who perform the Real-time reliability-related tasks of a Transmission Operator for ~~t~~Transmission Facilities at two or more locations;

4) ~~,~~Operating personnel of a Transmission Owner who have the capability to electronically control Transmission Facilities at two or more locations in real-time; or

5) Operating personnel of a Generator Operator who have the capability to electronically control ~~for~~ generation Facilities at two or more locations in real-time.

A. Introduction

1. Title: Cyber Security — Bulk Electric System (BES) Cyber System Categorization

2. Number: CIP-002-~~5.1a~~Y

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**Interchange Coordinator or Interchange Authority**~~

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-~~5.1a~~Y:

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.

5. Effective Dates: See "Project 2021-03 CIP-002 Transmission Owners Control Centers Implementation Plan"

~~1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

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

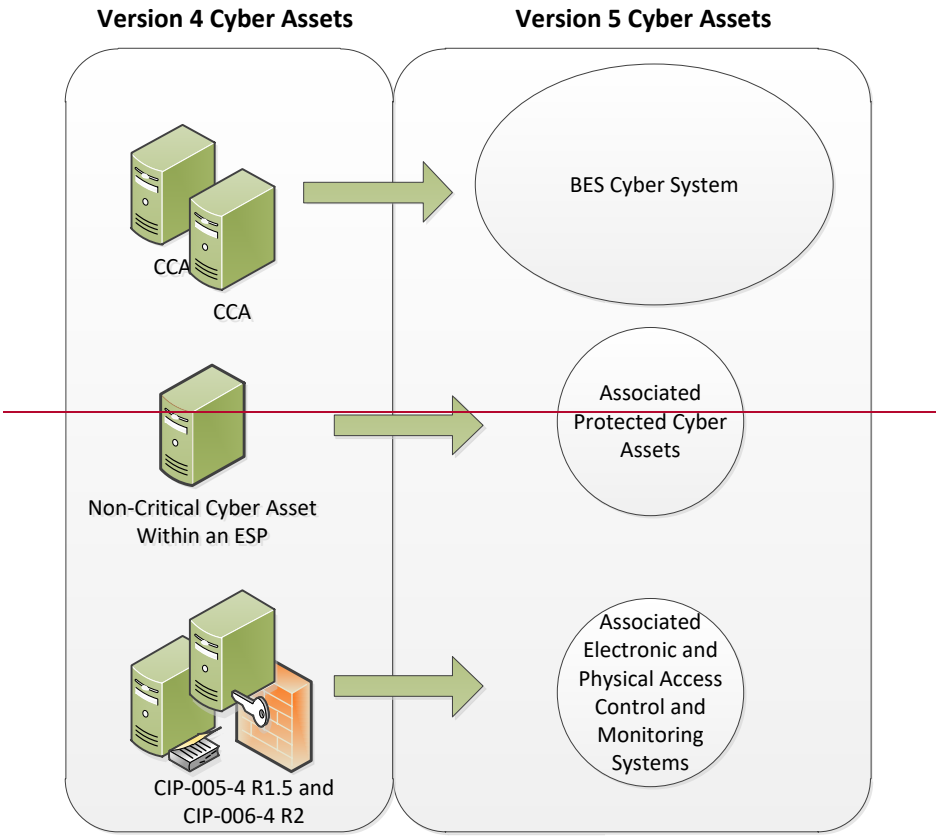
~~This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation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

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

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**BES Cyber Systems**~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

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

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System~~

~~boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

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

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

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

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic~~

~~Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

~~**Electronic Access Control or Monitoring Systems ("EACMS") –** Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~

~~**Physical Access Control Systems ("PACS") –** Examples include: authentication servers, card systems, and badge control systems.~~

~~**Protected Cyber Assets ("PCA") –** Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

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

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions. ~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

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

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

~~1.4. Additional Compliance Information~~

- ~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-~~5.1a~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities -with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-~~5.1a~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber	For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber ~~Assets~~Systems, more than 10 but less than or equal to 15 identified BES Cyber ~~Assets~~Systems have not been categorized or have been	Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities ~~-~~with more than a total of 100 high and medium impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-~~5.1a~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10- high or medium BES Cyber Systems have not been identified.	incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15- high or medium BES Cyber Systems have not been identified.	Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-~~5.1a~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-~~5.1a~~Y - Attachment 1

Impact Rating Criteria

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

1. High Impact Rating (H)

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

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

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

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

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

2. Medium Impact Rating (M)

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

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

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

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

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

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

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

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

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

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

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

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

Each BES Cyber System, not included in Section 1 above, used by and located at any of the following:

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

2.12. Each Control Center or backup Control Center ~~used to perform the functional obligations of the~~ , operated by a Transmission Operator or owned by a Transmission Owner, that is not already included in High Impact Rating (H~~),~~) above~~.~~, with an "aggregate weighted value" exceeding 6000 according to the table below and subject to the listed exclusion. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per characteristic" shown in the table for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line
<100 kV	100
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

Exclusion:

BES Transmission Lines monitored and controlled by the Control Center or backup Control Center may be excluded from the "aggregate weighted value" calculation if they are part of a local system that is operated at less than 300kV, where the net export from the local system does not exceed 75 MW during non-Energy Emergency Alert (EEA) conditions. The net export is based on the hourly integrated values for the most recent 12-month period.

~~2.12.~~**2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing

Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

3.5. ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES.

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

~~Guidelines and Technical Basis~~

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

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

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

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber~~

~~Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

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

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

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

~~Dynamic Response~~

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

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

~~Balancing Load and Generation~~

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

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

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

~~Controlling Frequency (Real Power)~~

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

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

~~Controlling Voltage (Reactive Power)~~

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

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

~~Managing Constraints~~

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

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

~~Monitoring and Control~~

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

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

~~Restoration of BES~~

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

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

~~Situational Awareness~~

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

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

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

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

Applicability to Distribution Providers

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

Requirement R1:

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

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

~~**Attachment 1**~~

~~**Overall Application**~~

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

- ~~When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~
- ~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~
- ~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~**High Impact Rating (H)**~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some~~

~~of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

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

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

~~Medium Impact Rating (M)~~

~~Generation~~

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

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

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

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

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

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

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

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

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

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

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

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

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

~~Transmission~~

~~*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.*~~

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

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

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

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

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

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

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

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

- ~~230 kV –> 700 MVA~~

- ~~345 kV –> 1,300 MVA~~

- ~~500 kV –> 2,000 MVA~~

- ~~765 kV –> 3,000 MVA~~

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

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate~~

~~connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~

- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~

- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

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

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~
2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

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

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

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

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

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

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

  ~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

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

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

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

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

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

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

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

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

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

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

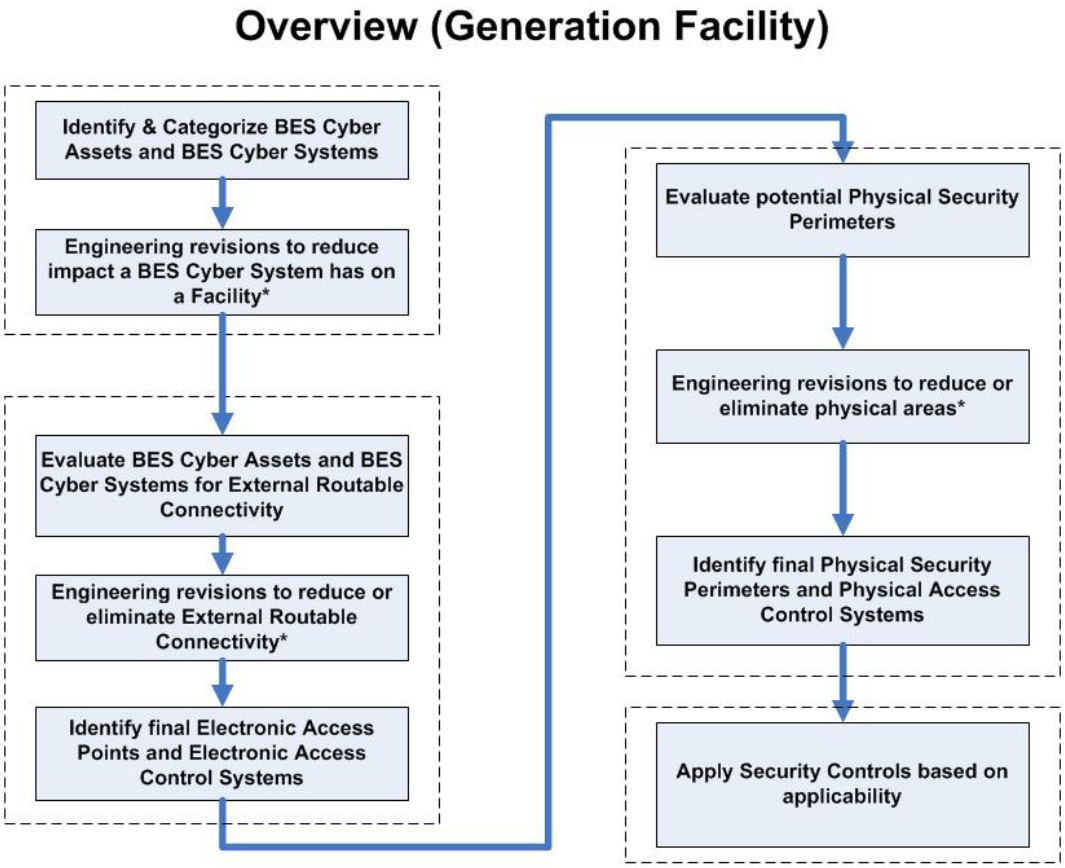
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific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

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

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

~~Use Case: CIP Process Flow~~

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



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

~~Rationale:~~

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

~~Rationale for R1:~~

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

~~Rationale for R2:~~

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

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.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
Y	TBD		

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~ ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~ ~~Attachment 1, Criterion 2.1~~ ~~2. Medium Impact Rating (M)~~ ~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~ ~~2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

Questions

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

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

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

Responses

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

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

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

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

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

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

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

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

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

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

Implementation Plan

Project 2021-03 CIP-002
Reliability Standard CIP-002-Y

Applicable Standard(s)

- Reliability Standard CIP-002-Y – Cyber Security -Bulk Electric System (BES) Cyber System Categorization

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security - BES Cyber System Categorization

Prerequisite Standard(s)

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

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Modified Terms in the NERC Glossary of Terms

This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Proposed Modified Definition(s):

Control Center – One or more rooms where a responsible entity hosts operating personnel to monitor and control the BES in real-time, as described below, including any spaces that house the Cyber Assets used by operating personnel to monitor and control the BES in real-time. Cyber

Assets used by operating personnel to monitor and control the BES in real-time are generally housed in a centralized location and exclude field assets such as remote terminal units.

(1) Operating personnel who perform the Real-time reliability-related tasks of a Reliability Coordinator;

(2) Operating personnel who perform the Real-time reliability-related tasks of a Balancing Authority;

(3) Operating personnel who perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations;

(4) Operating personnel of a Transmission Owner who have the capability to electronically control Transmission Facilities at two or more locations in real-time; or

(5) Operating personnel of a Generator Operator who have the capability to electronically control generation Facilities at two or more locations in real-time.

Background

Project 2021-03 addresses modifications to Reliability Standard CIP-002-5.1a to clarify the characterization of BES Cyber Systems associated with Control Centers used to perform the functional obligations of the Transmission Operator. Specifically, Project 2021-03 includes revisions to CIP-002 Criterion 2.12 in Attachment 1 and the Control Center definition. The proposed revisions to Attachment 1 address the categorization of Transmission Owner Control Centers performing the functional obligations of a Transmission Operator. These modifications resulted from recommendations from the CIP-002 Transmission Owner Control Center Field Test Report.[1]

General Considerations

This Implementation Plan includes phased-in implementation dates for Criterion 2.12 of CIP-002-Y, Attachment 1. The phased-in implementation dates allow Responsible Entities[2] a longer implementation period if the revisions to the criterion would result in a higher impact level categorization of a BES Cyber System.

Effective Date and Phased-In Compliance Dates

The effective date for proposed Reliability Standard CIP-002-Y and the modified definition is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion of it), the additional time for compliance with that section is specified below. The phased-in implementation date for those particular sections is the date that Responsible

[1] The final field test report is available at https://www.nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03_CIP-002_TOCC_Field_Test_Final_Report_01262023.pdf.

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

Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Reliability Standard CIP-002-Y – Cyber Security – BES Cyber System Categorization
Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is three (3) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is three (3) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Dates for CIP-002-Y

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in CIP-002-Y, Requirement R2 within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

Phased-in Implementation Date for CIP-002-Y, Requirement R1, Attachment 1 Criterion 2.12

If the revisions to Criterion 2.12 of Attachment 1 to CIP-002-Y result in a higher impact level categorization of a BES Cyber System, the Responsible Entity shall not be required to identify that BES Cyber System as that higher categorization nor apply the requirements throughout the CIP standards applicable to that higher categorization until 24 months after the effective date of CIP-002-Y. Until that time, the Responsible Entity shall continue to identify that BES Cyber System consistent with its existing categorization under CIP-002-5.1a, Requirement R1, Part 1.3.

Planned or Unplanned Changes

The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5.1a shall apply to CIP-002-Y. The Implementation Plan associated with CIP-002-5.1a[3] provided as follows with respect to planned and unplanned changes (with conforming changes to the version numbers of the standard):

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-Y, Requirement R2. For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-Y, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

[3] The Implementation Plan associated with CIP-002-5.1a is available at https://www.nerc.com/pa/Stand/Project%20200806%20Cyber%20Security%20Order%20706%20DL/Implementation_Plan_clean_4_(2012-1024-1352).pdf.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-5.1a Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-Y, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-Y, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-Y, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-5.1a Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium impact BES Cyber Systems

Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes)	24 months

Control Center Definition

Where approval by an applicable governmental authority is required, the definition shall become effective on the first day of the first calendar quarter that is three (3) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-002-Y, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter that is three (3) months after the date that Reliability Standard CIP-002-Y is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

Reliability Standard CIP-002-5.1a

Reliability Standard CIP-002-5.1a shall be retired immediately prior to the effective date of Reliability Standard CIP-002-Y in the particular jurisdiction in which the revised standard is becoming effective.

SPSEG Process Improvement Recommendations Work Plan Status Report

Action
Inform

Summary
At its March 22, 2023 meeting, 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 that do not conform to the SPM	SCPS	In Process
2	Provide guidance to drafting teams on the role of the SAR in standards development process	• Incorporate guidance into drafting team reference manual, other applicable drafting team resources • Incorporate into work of the SCCG SPSEG recommendation review of SAR form	SCPS, NERC staff SC leadership, SCCG	In Process 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	In Process Complete
4	Implement changes in administration			

[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.

	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	In Process In Process
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	In Process
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	• Review and update drafting team reference	SCPS	In Process

	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	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, NERC staff	In Process

NERC Legal and Regulatory Update – Reliability Standards
August 8, 2023 – September 10, 2023

NERC FILINGS TO FERC SUBMITTED SINCE LAST SC UPDATE

FERC Docket No.	Filing Description	FERC Submittal Date
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.	8/16/2023

FERC ISSUANCES SINCE LAST SC UPDATE

FERC Docket No.	Issuance Description	FERC Issuance Date
	None	

ANTICIPATED UPCOMING FILINGS

FERC Docket No.	Filing Description	Anticipated Filing Date
TBD	Petition for approval of ROP Section 300 and Standard Processes Manual	9/15/2023
RD20-2-000	CIP SDT Schedule Compliance Filing	9/15/2023
TBD	Petition for approval of modifications to IRO-010 and TOP-003	9/15/2023
RR10-1-000; RR13-3-000	Annual Report of NERC on Wide-Area Analysis of Technical Feasibility Exceptions (TFEs)	9/28/2023

Standards Committee Expectations

Approved by Standards Committee January 12, 2012

Background

Standards Committee (SC) members are elected by members of their segment of the Registered Ballot Body, to help the SC fulfill its purpose. According to the Standards Committee Charter, the SC's purpose is:

> *In compliance with the NERC Reliability Standards Development Procedure, the Standards Committee manages the NERC standards development process for the North American-wide reliability standards with the support of the NERC staff to achieve broad bulk power system reliability goals for the industry. The Standards Committee protects the integrity and credibility of the standards development process.*

The purpose of this document is to outline the key considerations that each member of the SC must make in fulfilling his or her duties. Each member is accountable to the members of the Segment that elected them, other members of the SC, and the NERC Board of Trustees for carrying out their responsibilities in accordance with this document.

Expectations of Standards Committee Members

1. SC members represent their segment, not their organization or personal views. Each member is expected to identify and use mechanisms for being in contact with members of the segment in order to maintain a current perspective of the views, concerns, and input from that segment. NERC can provide mechanisms to support communications if an SC member requests such assistance.
2. SC members base their decisions on what is best for reliability and must consider not only what is best for their segment, but also what is in the best interest of the broader industry and reliability.
3. SC members should make every effort to attend scheduled meetings, and when not available are required to identify and brief a proxy from the same segment. SC business cannot be conducted in the absence of a quorum, and it is essential that each SC member make a commitment to being present.
4. SC members should not leverage or attempt to leverage their position on the SC to influence the outcome of standards projects.
5. The role of the SC is to manage the standards process and the quality of the output, not the technical content of standards.

Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 11th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." The vote is subject to a 2/3 majority approval. Also, any member may call the question. This motion is not debatable. The vote is subject to a 2/3 vote.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The “seconder” is not recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee “owns” the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent The standard practice.	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.