BEFORE THE
NOVA SCOTIA ENERGY BOARD
OF THE PROVINCE OF NOVA SCOTIA

North American Electric Reliability Corporation	**)**

FIRST QUARTER 2026 APPLICATION FOR APPROVAL OF RELIABILITY STANDARDS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Senior Counsel
Marisa Hecht
Senior Counsel
Alain Rigaud
Associate Counsel
North American Electric Reliability Corporation
1401 H Street NW Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net
marisa.hecht@nerc.net
alain.Rigaud@nerc.net

Counsel for the North American Electric Reliability Corporation

May 28, 2026

I. NOTICE AND COMMUNICATIONS 3

II. REQUEST FOR APPROVAL OF RELIABILITY STANDARDS 4

A. BACKGROUND: NERC QUARTERLY FILING OF PROPOSED RELIABILITY STANDARDS .. 4

B. OVERVIEW OF NERC RELIABILITY STANDARDS DEVELOPMENT PROCESS 6

C. DESCRIPTION OF PROPOSED RELIABILITY STANDARDS, FIRST QUARTER 2026 7

1. MOD-032-2; IRO-010-6; TOP-003-8; MOD-033-3; MOD-026-2 - Inverter-based Resources and Generators Modeling Reliability Standards 9

2. CIP-002-7; CIP-003-10; CIP-004-8; CIP-005-8; CIP-006-7.1; CIP-007-7.1 CIP-008-7.1; CIP-009-7.1; CIP-010 -5; CIP-011-4.1; CIP-013-3 - Virtualization Reliability Standards 22

BES Cyber System: 36

3. CIP-003-11 (Cyber Security - Security Management Controls): 36

4. CIP-002-8 (Cyber Security-BES Cyber System Categorization) 39

5. BAL-007-1.1 Errata (Near-Term Energy Reliability Assessments) 42

D. DESCRIPTION OF PROPOSED NERC GLOSSARY DEFINITIONS, SECOND QUARTER 2024 42

6. Reporting ACE Definitions 43

III. CONCLUSION 49

Exhibit A	**Exhibit A-1:** Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026
	Exhibit A-2: Informational Summary of Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026
	Exhibit A-3: Reliability Standards Filed for Approval in First Quarter 2026
	Exhibit A-4: Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024
	Exhibit A-5: Informational Summary of Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024
	Exhibit A-6: Definitions Filed for Approval in Second Quarter 2024
Exhibit B	List of Currently Effective NERC Reliability Standards
Exhibit C	Updated Glossary of Terms Used in NERC Reliability Standards

BEFORE THE
NOVA SCOTIA ENERGY BOARD
OF THE PROVINCE OF NOVA SCOTIA

North American Electric Reliability Corporation	**)**

FIRST QUARTER 2026 APPLICATION
FOR APPROVAL OF RELIABILITY STANDARDS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC") hereby submits to the Nova Scotia Energy Board ("NSEB") an application for approval of NERC Reliability Standards approved by the United States Federal Energy Regulatory Commission ("FERC") during the first quarter of 2026 (from January 1, 2026 through March 31, 2026). NERC requests that the Reliability Standards approved by FERC in the first quarter of 2026 be made mandatory and enforceable for users, owners, and operators of the Bulk-Power System ("BPS") within the Province of Nova Scotia. This application also submits for approval the retirement of certain Reliability Standards which were approved by FERC in the first quarter of 2026.

In addition, NERC submits for approval, to the extent necessary, new, revised, and retired definitions of terms related to the calculation of Reporting Area Control Error, or Reporting ACE, which were approved by FERC in the second quarter of 2024. NERC originally developed these definition proposals as part of a definition-only revision project, where there was no new or revised Reliability Standard being proposed. Upon completing a recent review of its records, NERC discovered that it inadvertently failed to identify these definition proposals in a standalone application for approval in the quarter following FERC approval in 2024. These terms have been

provided to Nova Scotia by NERC with each subsequent version of the NERC Glossary of Terms, which has been included with NERC's quarterly filings.[1]

In support of this request, NERC submits the following information: (i) a table listing the United States effective date of each Reliability Standard applicable to Nova Scotia that was approved by FERC in the first quarter of 2026 (**Exhibit A-1**); (ii) an informational summary of the Reliability Standards applicable to Nova Scotia that were approved by FERC in the first quarter of 2026, including each standard's purpose, applicability, as well as the date that NERC filed the Reliability Standard with FERC and the date that FERC approved the Reliability Standard (**Exhibit A-2**); (iii) the Reliability Standards approved by FERC in the first quarter of 2026 (**Exhibit A-3**); (iv) an updated list of the currently effective NERC Reliability Standards as approved by FERC (**Exhibit B**); (v) the updated *Glossary of Terms Used in NERC Reliability Standards* ("*NERC Glossary*") (**Exhibit C**),[2] and (vi) Definitions Filed for Approval in Second Quarter 2024 **(Exhibit A-6)**.

I. NOTICE AND COMMUNICATIONS

[1] *Petition of the N. Am. Elec. Reliability Corp. for Approval of New, Revised, and Retired Definitions of Terms Used in NERC Reliability Standards*, Docket No. RD24-6-000 (Mar. 8, 2024); *Order Approving New and Revised Definitions of Terms Used in Reliability Standards*, Docket No. RD24-6-000 (Apr. 29, 2024).

[2] The list of Reliability Standards and the *NERC Glossary* in **Exhibit B** and **Exhibit C**, respectively, were generated on or around the date of this filing, and, given the quarterly schedule on which this application is filed, these lists may include standards and definitions that became effective or were approved after the final day of the previous quarter. Only those standards and definitions highlighted for NSEB in the present quarterly application and all previous applications should be considered for purposes of this application.

Notices and communications regarding this application may be addressed to:

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
sarah.crawford@nerc.net

II. REQUEST FOR APPROVAL OF RELIABILITY STANDARDS

A. Background: NERC Quarterly Filing of Proposed Reliability Standards

Pursuant to Section 215 of the Federal Power Act ("FPA"),[3] NERC is certified by FERC as the Electric Reliability Organization ("ERO") in the United States.[4] Under FPA Section 215, the ERO is charged with developing and enforcing mandatory Reliability Standards in the United States, subject to FERC approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the BPS in the United States will be subject to FERC-approved Reliability Standards. Section 215(d)(5) of the FPA authorizes FERC to order the ERO to submit a new or modified Reliability Standard and Section 39.5(a) of FERC's regulations requires the ERO to file for FERC approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective in the United States. Some or all of NERC's Reliability Standards are also mandatory in the Canadian provinces of Alberta, British Columbia, Manitoba, New

[3] 16 U.S.C. § 824o (entrusting FERC with the duties of approving and enforcing rules in the U.S. to ensure the reliability of the nation's Bulk-Power System, and with the duties of certifying an Electric Reliability Organization to develop mandatory and enforceable Reliability Standards, subject to FERC review and approval).

[4] *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

Brunswick, Nova Scotia, Ontario, Québec, and Saskatchewan.

NERC entered into a Memorandum of Understanding ("MOU") with the Nova Scotia Utility and Review Board ("NSUARB",[5] now known as the Nova Scotia Energy Board or "NSEB") and a separate MOU with Nova Scotia Power Inc. ("NSPI") and the Northeast Power Coordinating Council, Inc. ("NPCC"),[6] to provide reliability services to Nova Scotia. These MOUs became effective on December 22, 2006 and May 11, 2010, respectively. The December 22, 2006 MOU memorialized the relationship between NERC and the NSUARB that was formed to improve the reliability of the North American BPS. The May 11, 2010 MOU sets forth the mutual understanding of NERC, NSPI, and NPCC regarding the approval and implementation of NERC Reliability Standards and NPCC Regional Reliability Criteria in Nova Scotia and other related matters.

On June 30, 2010, NERC submitted its first set of Reliability Standards and the *NERC Glossary* to the NSUARB, and on July 20, 2011, the NSUARB issued a decision approving these documents.[7] In that decision, the NSUARB approved a quarterly review process for considering new and amended NERC Reliability Standards and criteria[8] and ordered that "applications will not be processed by the Board until [FERC] has approved or remanded the standards in the United States."[9] The NSUARB Decision also stated that NSUARB approval is not required for the Violation Risk Factors and Violation Severity Levels associated with proposed Reliability

---

5 *See* Memorandum of Understanding between Nova Scotia Utility and Review Board and North American Electric Reliability Corporation (signed Dec. 22, 2006).

6 *See* Memorandum of Understanding between Nova Scotia Power Incorporated and the Northeast Power Coordinating Council, Inc. and the North American Electric Reliability Corporation (signed May 11, 2010).

7 *In the Matter of an Application by North American Electric Reliability Corporation for Approval of its Reliability Standards, and an application by Northeast Power Coordinating Council, Inc. for Approval of its Regional Reliability Criteria*, NSUARB-NERC-R-10 (July 20, 2011) [hereinafter NSUARB Decision].

8 *Id.* at P 30.

9 *Id.*

Standards, but the NSUARB noted that it will accept Violation Risk Factors and Violation Severity Levels as guidance.[10]

Based on the NSUARB Decision, NERC applications to the NSUARB, now NSEB, only request approval for those Reliability Standards and *NERC Glossary* definitions approved by FERC during the previous quarter. NERC does not seek formal approval of Violation Risk Factors and Violation Severity Levels associated with the Reliability Standards submitted in its quarterly applications. Rather, for informational purposes and for guidance, NERC provides a link to the FERC-approved Violation Risk Factors and Violation Severity Levels associated with NERC Reliability Standards.[11] NERC does not include in its applications the full developmental record for the standards, which consists of the draft standards, comments received, responses to the comments by the drafting teams, and the full voting record, because the record for each standard may consist of several thousand pages. NERC will make the full developmental records available to the NSEB or other interested parties upon request.[12]

B. Overview of NERC Reliability Standards Development Process

NERC Reliability Standards define the requirements for reliably planning and operating the North American BPS. These standards are developed by industry stakeholders using a balanced, open, fair, and inclusive process managed by the NERC Standards Committee. The Standards Committee is facilitated by NERC staff and comprised of representatives from ten electricity stakeholder segments. Stakeholders, through a balloting process, approve the Reliability

---

[10] *Id.* at P 33.

[11] NERC's Violation Risk Factors Matrix and Violation Severity Levels Matrix are available at https://www.nerc.com/pa/Stand/Pages/default.aspx. See the left-hand side of webpage for downloadable documents.

[12] The full record of development for each standard is available on NERC's website as an exhibit to the petition filed with FERC. These petitions are available at https://www.nerc.com/who-we-are/regulatory/filings-to-ferc.

Standards prior to the standards being adopted by the NERC Board of Trustees and approved by applicable governmental authorities.

NERC develops Reliability Standards and associated definitions in an open, inclusive, balanced, and fair process in accordance with Section 300 (Reliability Standards Development) and Appendix 3A (Standard Processes Manual) of its Rules of Procedure.[13] The *NERC Glossary*, most recently updated April 1, 2026, contains each term that is defined for use in one or more of NERC's continent-wide or regional Reliability Standards approved by the NERC Board of Trustees. Since the *NERC Glossary* was first approved in 2007, FERC has approved new defined terms and revisions to the definitions of existing terms developed through the standard development process, as well as the retirement of previously effective terms and definitions. While defined terms typically accompany the new or revised Reliability Standards that will use those terms, NERC has on occasion proposed new or revised defined terms independent of a proposed Reliability Standard.

C. Description of Proposed Reliability Standards, First Quarter 2026

As provided in the table below, during the first quarter of 2026, FERC issued five orders approving the following Reliability Standards and definitions:

- Inverter-Based Resources and Generators Modeling Reliability Standards: (1) MOD-032-2 (Data for Power System Modeling and Analysis); (2) IRO-010-6 (Reliability Coordinator Data and Information Specification and Collection); (3) TOP-003-8 (Transmission Operator and Balancing Authority Data Information Specification and Collection); (4) MOD-033-3 (Steady-State and Dynamic System Model Validation); (5) MOD-026-2 (Verification and Validation of Dynamic Models and Data); and definitions of Distributed Energy Resources (DER), Model Validation, and Model Verification.[14]

[13] The NERC *Rules of Procedure* are available at https://www.nerc.com/who-we-are/rules-of-procedure.

[14] *Order Approving Inverter-Based Resources and Generators Modeling Reliability Standards,* 194 ¶ 61,125 (2026).

- CIP-003-11 (Cyber Security – Security Management Controls)[15]

- Virtualization Reliability Standards: (1) CIP-002-7 (Cyber Security-BES Cyber System Categorization); (2) CIP-003-10 (Cyber Security-Security Management Controls); (3) CIP-004-8 (Cyber Security-Personnel & Training); (4) CIP-005-8 (Cyber Security-Electronic Security Perimeters(s)); (5) CIP-006-7.1 (Cyber Security-Physical Security of the BES Cyber Systems); (6) CIP-007-7.1 (Cyber Security-Systems Security Management); (7) CIP-008-7.1 (Cyber Security-Incident Reporting and Response Planning; (8) CIP-009-7.1 (Cyber Security-Recovery Plans for BES Cyber Systems); (9) CIP-010-5 (Cyber Security – Configuration Change Management and Vulnerability Assessments); (10) CIP-011-4.1 (Cyber Security – Information Protection); and (11) CIP-013-3 (Cyber Security – Supply Chain Risk Management). The approved definitions are: (1) Cyber System, (2) Management Interface; (3) Shared Cyber Infrastructure; (4) Virtual Cyber Asset; (5) BES Cyber Asset; (6) BES Cyber System; (7) BES Cyber System Information; (8) CIP Senior Manager; (9) Cyber Asset; (10) Cyber Security Incident; (11) Electronic Access Control or Monitoring Systems; (12) Electronic Access Point, External Routable Connectivity; (13) Electronic Security Perimeter; (14) Interactive Remote Access; (15) Intermediate System; (16) Physical Access Control Systems; (17) Physical Security Perimeter; (18) Protected Cyber Asset; (19) Removable Media; (20) Reportable Cyber (21) Security Incident; and (22)Transient Cyber Asset.[16]

- CIP-002-8 (Cyber Security-BES Cyber System Categorization)[17]

- BAL-007-1 (Near-Term Energy Reliability Assessments) Errata[18]

No other Reliability Standards applicable to Nova Scotia were approved by FERC during the first quarter of 2026.

---

15 *Critical Infrastructure Protection Reliability Standard CIP -003-11 – Cyber Security-Security Management Controls*, Order No. 918, 194 FERC ¶ 61,210 (2026) [hereinafter Order No. 918].

16 *Virtualization Reliability Standards*, Order No. 919, 194 ¶ 61,209 (2026) [hereinafter Order No. 919].

17 *N. Am. Elec. Reliability Corp.*, Docket No. RD25-8-000 (Mar. 19, 2026) (letter order).

18 *N. Am. Elec. Reliability Corp.*, Docket No. RD26-4-000 (Mar. 26, 2026) (delegated letter order).

Reliability Standards

Reliability Standard	Effective Date
Modeling, Data, and Analysis (MOD)	
MOD-032-2*	4/1/2028
MOD-033-3	4/1/2026
MOD-026-2	4/1/2026
Interconnection Reliability Operations and Coordination (IRO)	
IRO-010-6*	4/1/2029
Transmission Operations (TOP)	
TOP-003-8*	4/1/2029
Critical Infrastructure Protection (CIP)	
CIP-003-10*	7/1/2028
CIP-003-11*	7/1/2029
CIP-004-8*	7/1/2028
CIP-005-8*	7/1/2028
CIP-006-7.1*	7/1/2028
CIP-007-7.1*	7/1/2028
CIP-008-7.1*	7/1/2028
CIP-009-7.1*	7/1/2028
CIP-010-5*	7/1/2028
CIP-011-4.1*	7/1/2028
CIP-013-3*	7/1/2028
CIP-002-7**	7/1/2028
CIP-002-8* **	7/1/2028
Resource and Demand Balancing (BAL)	
BAL-007-1*	4/1/2027

*At the time of this filing, the standards marked with an asterisk are not yet effective but have been approved by FERC and have a future mandatory effective date.

** On March 19, 2026, FERC issued orders that approve revisions to two versions of Reliability Standard CIP-002, CIP-002-7 and CIP-002-8. The revisions that were first proposed in CIP-002-7 were carried forward and included in Reliability Standard CIP-002-8 and accounted for in the CIP-002-8 Implementation Plan. As a result, CIP-002-8 was designed to replace CIP-002-7 on its effective date if both versions were approved by FERC on or near the same date.

1. *MOD-032-2; IRO-010-6; TOP-003-8; MOD-033-3; MOD-026-2 - Inverter-based Resources and Generators Modeling Reliability Standards*

On February 19, 2026, FERC issued an order approving Reliability Standards MOD-032-2 (Data for Power System Modeling and Analysis), IRO-010-6 (Reliability Coordinator Data and Information Specification and Collection), TOP-003-8 (Transmission Operator and Balancing Authority Data Information Specification and Collection), MOD-033-3 (Steady-State and

Dynamic System Model Validation), MOD-026-2 (Verification and Validation of Dynamic Models and Data), as well as the associated violation risk factors and violation severity levels, implementation plans, and the definitions of the terms Distributed Energy Resource ("DER"), Model Validation, and Model Verification.

Reliability Standards MOD-032-2, IRO-010-6, TOP-003-8, MOD-033-3 and MOD-26-2 are responsive to FERC Order No. 901, in which FERC directed NERC to submit new or revised standards addressing Inverter-Based Resource ("IBR") data sharing and model validation for IBRs,[19] including IBRs that are connected to the BPS as well as IBRs that are connected to a distribution system but in the aggregate have a material impact on the BPS. FERC directed NERC to address specific reliability gaps because the existing Reliability Standards do not adequately address the reliability risks posed by the increasing numbers of IBRs connecting to the BPS. In Order No. 901, FERC directed NERC to develop new and revised Reliability Standards to address the following four topic areas of IBR issues: (1) data sharing; (2) data and model validation, (3) planning and operational studies; and (4) performance requirements.[20]

To respond to Order No. 901, NERC developed a work plan that includes the following four milestones:

- Milestone 1: Submission of Order No. 901 Work Plan (completed: January 17, 2024).
- Milestone 2: Development and Filing of Reliability Standards to Address Disturbance Monitoring Requirements, Performance Requirements and Post-Event Performance Validation for Registered IBRs (completed: November 4, 2024).
- Milestone 3: Development and Filing of Reliability Standards to Address Data sharing and Model Validation for all IBRs (completed: November 4, 2025).

[19] *Reliability Standards to Address Inverter-Based Resources,* Order No. 901, 185 FERC ¶ 61,042 at P 229 (2023) [hereinafter Order No. 901].

[20] *Id.* at PP 1, 5, 53.

- Milestone 4: Development and Filing of Reliability Standards to Address Planning and Operational Studies Requirements for all IBRs (completion: November 4, 2026).

As discussed in detail below, Reliability Standards MOD-032-2; IRO-010-6; TOP-003-8; MOD-033-3; and MOD-026-2 address critical IBR reliability issues in accordance with Milestone 3. Reliability Standards MOD-032-2, IRO-010-6, and TOP-003-8, establish modeling and data sharing requirements that provide sufficient IBR and DER model data and parameters to assure accurate representations of IBR and DER performance within system models. Reliability Standard MOD-033-3 establishes a more comprehensive and thorough System Model Validation process to ensure IBRs and DERs, which make up an increasing part of the resource mix of the BPS, are included in the process. In addition, Reliability Standard MOD-026-2 enhances the Model Validation and Model Verification processes to ensure that positive sequence dynamic and electromagnetic transient ("EMT" models of IBRs accurately reflect real operation behavior of in-service equipment. This is accomplished by making sure that models, particularly of IBRs, used in operational and planning interconnection studies more accurately represent how these facilities behave during normal periods and disturbance events, and reduce the risk of model-based forecasts being different from real outcomes.

MOD-032-2 (Data for Power System Modeling and Analysis): The purpose of Reliability Standard MOD-032-2 is "To establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system." The revised standard continues to apply to the Balancing Authority, Generator Owner, Planning/Planning Coordinator, Resource Planner, Transmission Owner, Transmission Planner, and Transmission Service Provider, as in currently effective Reliability Standard MOD-032-1. Reliability Standard MOD-032-2 removes the Load

Serving Entity, an applicable functional entity category that is no longer registered for mandatory Reliability Standards compliance purposes. Reliability Standard MOD-032-2 adds the Distribution Provider as the functional entity that would provide the data formerly associated with the Load Serving Entity in Reliability Standard MOD-032-1.

Reliability Standard MOD-032-2 Requirement R1 requires each Planning Coordinator and each of its Transmission Planners to jointly develop steady-state, dynamics, and short circuit modeling data requirements and reporting procedures for the Planning Coordinator's planning area. Responsible entities are then required to provide the data under Requirement R2.

- Requirement R1 Part 1.1 requires the inclusion of data listed in Attachment 1, along with the entity responsible for providing each required item. Attachment 1 defines the information that is required to effectively model the interconnected transmission system for transmission planning studies, with three columns addressing data and information needed for steady-state, dynamics, and short circuit analyses. The modifications to Requirement R1 Part 1.1 require the Planning Coordinator and its Transmission Planners to identify the entity or category of entities responsible for the data items listed in Attachment 1.

- Requirement R1 Part 1.2, relating to specifications for data format, level of detail, case types or scenarios to be modeled, and data submission schedules, is carried forward unchanged from the currently effective version.

- Requirement R1 Part 1.3, relating to specifications for distributing or posting data requirements and reporting procedures, is also carried forward unchanged.

- Requirement R1 Part 1.4 is a new requirement part that addresses required specifications for dynamic model submissions. Requirement R1 Part 1.4 includes requirements for the Planning Coordinator/Transmission Planner to specify submission of standard library dynamic models, user-defined models, or both. Requirement R1 Part 1.4 also provides the Planning Coordinator/Transmission Planner with the authority to require submission of both model types.

- Requirement R1 Part 1.4.2.1 requires each Planning Coordinator and Transmission Planner accepting user-defined models to provide their user-defined model requirements to other Planning Coordinators and Transmission Planners within the Interconnection upon request.

Attachment 1, referenced in Requirement R1, defines the information that is required to effectively model the interconnected transmission system for transmission planning studies. Attachment 1 has three columns addressing data and information needed for steady-state, dynamics, and short circuit analyses. As revised, Attachment 1 replaces all references to the Load-Serving Entity as a typical entity responsible for providing certain data with the Distribution Provider. Attachment 1 also reflects several revisions to improve data that is collected for IBRs, including BPS connected IBRs owned by Generator Owners registered with NERC for mandatory compliance purposes (referred to as "registered IBRs" in Order No. 901) and BPS IBRs that fall below the threshold that would require the owner to register with NERC (referred to as "unregistered IBRs" in Order No. 901). Attachment 1 also reflects several revisions to improve the data collected for DERs, including IBR-DER and other DER, that in the aggregate can affect the reliability of the Bulk-Power System. To improve Attachment 1 as it relates to DER data, new item 9 in the steady-state column addresses aggregate DER data, including location, Real Power capability, and DER type as required items.

Reliability Standard MOD-032-2 Requirement R2 establishes requirements for Balancing Authorities, Distribution Providers, Generator Owners, Resource Planners, Transmission Owners, and Transmission Service Providers to provide data according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1. Requirement R2 revises the currently effective requirement to address the provision of estimated data and the submission of models deemed generally unacceptable for studies. Requirement R2 replaces the Load Serving Entity with the Distribution Provider, consistent with changes made to the Applicability of the standard and Attachment 1 discussed in previous sections.

- Requirement R2 Part 2.1 is a new requirement part addressing how registered entities would provide estimated data for resources owned by unregistered entities if they are unable to gather the actual data. Requirement R2 Part 2.1 also addresses the estimation of aggregate DER data, regardless of resource type.

- Requirement R2 Part 2.2 is a new requirement part intended to confirm the relationship between Reliability Standard MOD-032-2 Reliability Standard MOD-026-2. Requirement R2 Part 2.2 requires the model submitted by the functional entity be the model that was verified and validated (and accepted by the Transmission Planner) in accordance with MOD-026, if available.

- Requirement R2 Part 2.3 provides that entities providing any model included on the Unacceptable Models List maintained by the ERO shall provide a technical justification supporting its use.

Reliability Standard MOD-032-2 Requirement R3 addresses the identification of technical concerns with data submitted under Requirement R2. Revisions to replace the Load Serving Entity with the Distribution Provider are consistent with other revisions to the standard discussed in previous sections. The addition of the phrase "responsive to the technical concern" in Requirement R3 Part 3.1 supports the goal of Requirement R3, which is to resolve technical concerns that are identified by the Planning Coordinator or Transmission Planner with submitted data or models.

Reliability Standard MOD-032-2 Requirement R4 is carried forward unchanged from the currently effective standard.

IRO-010-6 (Reliability Coordinator Data and Information Specification and Collection) and TOP-003-8 (Transmission Operator and Balancing Authority Data Information Specification and Collection): The titles and purposes of both standards remain unchanged. Reliability Standard IRO-010-6 remains applicable to the Reliability Coordinator, Balancing Authority, Generator Owner (to include newly-registered Generator Owners under the expanded NERC Registry criteria), Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider. Reliability Standard TOP-003-8 remains applicable to the Transmission Operator,

Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider.

Reliability Standards IRO-010-6 and TOP-003-8 help ensure that IBR-specific data and parameters are addressed in Reliability Coordinator, Balancing Authority, and Transmission Operator data specifications. Both standards have broad requirements that allow the Reliability Coordinator, Transmission Operator, or Balancing Authority to request data and information needed to support their respective operations planning, analysis, or Real-time activities from generation and storage resources, including IBR.

To address the relevant directives in Order No. 901, Reliability Standards IRO-010-6 and TOP-003-8 add "Inverter-based Resource (IBR) - specific data and parameters" to the list of information the Reliability Coordinator, Transmission Operator, and Balancing Authority must address in its documented data specifications. Reliability Standard IRO-010-6 includes these revisions in Requirement R1 Part 1.1. Corresponding revisions in Reliability Standard TOP-003-8 are located in Requirement R1 Part 1.1 and Requirement R2 Part 2.1. These revisions address the Order No. 901 directives related to the sharing of IBR data with Reliability Coordinators, Transmission Operators, and Balancing Authorities, as well as directives addressing IBRs in operations models. The phrase "IBR-specific data and parameters" is intended to reflect what FERC describes in Order No. 901 as "IBR models that accurately reflect the behavior of IBRs during steady state, short-circuit, and dynamic conditions." The relocation of the phrase "as deemed necessary by the Reliability Coordinator" is intended to provide for clarity in the requirement.

To create the uniform framework for modeling across planning and operations, Reliability Standards IRO-010-6 and TOP-003-8 also add that operations data specifications have

"requirements for necessary model submissions to be consistent with the model submitted for planning purposes, subject to modifications for operations purposes, as applicable." Reliability Standard IRO-010-6 includes these revisions in Requirement R1 Part 1.5.3; corresponding revisions in Reliability Standard TOP-003-8 are located in Requirement R1 Part 1.5.3 and Requirement R2 Part 2.5.3. Models submitted for planning purposes are typically made in accordance with the MOD-032 standard, though additional standards or regional requirements may apply. Some modifications to these planning models may be necessary to reflect considerations for operations. For example, simulation time constraints in an online operations environment may warrant a reduced model structure complexity. Such models may differ from, but should still be consistent with, more complex modeling that is submitted under MOD-032. As another example, consistent models would not be appropriate if an update was made to a planning model for known pending changes, which should not be reflected in the operations models prior to implementation. The inclusion of "as applicable" allows for variation as necessary for application in the operations horizon as well as to reflect that entities may determine when such models are needed for their operations planning and Real-time functions.

MOD-033-3 (Steady-State and Dynamic System Model Validation): The purpose of Reliability Standard MOD-033-3 is: "To establish a process for system model validation to facilitate achieving and maintain model accuracy." The title remains unchanged and Reliability Standard MOD-033-3 continues to apply to the Planning Authority/Planning Coordinator, Reliability Coordinator, and Transmission Operator. Transmission Planners are excluded from Reliability Standard MOD-033-3 because each Transmission Planner is either its own Planning Coordinator or within a Planning Coordinator's footprint in accordance with NERC Registry Criteria.

Requirement R1 requires each Planning Coordinator to develop and implement a documented Model Validation process for the planning models in the Planning Coordinator's portion of the existing System against actual System behavior. Under Requirement R1, the planning models include any registered IBRs, IBRs that are not DERs and do not meet NERC's registration criteria "unregistered IBRs", or aggregated DERs present in the existing System consistent with modeling data requirements in Reliability Standard MOD-032 and in accordance with the System Model Validation directives in Order No. 901.

- Requirement R1, Part 1.1 addresses periodic validation of steady-state System model by requiring comparison of power flow simulation performance to actual measured System behavior using relevant real-time data sources such as state estimator cases or real-time telemetered data.

- Requirement R1 Part 1.2 addresses periodic validation of dynamic data within the Planning Coordinator's portion of the System.

- Requirement R1 Part 1.3 preserves that the Planning Coordinator is responsible for developing guidelines determining the required accuracy when comparing simulation results against actual System behavior. The revisions also clarify that the guidelines should include unacceptable differences in performance for generating facilities in the planning System models.

- Requirement R1 Part 1.4 carries forward the requirement for the Planning Coordinator to develop guidelines to resolve any unacceptable differences that are identified under Part 1.3 of its Model Validation process.

Requirement R2 requires the Reliability Coordinator and Transmission Operator to provide actual System behavior data to any Planning Coordinator performing Model Validation under Requirement R1 within 30 days of a written request. This provides a mechanism for Planning Coordinators to obtain actual System behavior data from the Reliability Coordinators and Transmission Operators that are required to perform System Model Validation.

MOD-026-2 (Verification and Validation of Dynamic Models and Data): The title of Reliability Standard MOD-026-2 is – Verification and Validation of Dynamic Models and Data.

The stated purpose of the standard is: "To verify and validate that the dynamic models and associated parameters used to assess Bulk Electric System (BES) reliability represent the in-service equipment of Bulk Power System (BPS) facilities including generating facilities, transmission connected dynamic reactive resources, and high-voltage direct current (HVDC) systems." Reliability Standard MOD-026-2 would be applicable to Generator Owners,[21] Transmission Owners, Planning Coordinators, and Transmission Planners.

Reliability Standard MOD-026-2 advances reliability by enhancing the Model Validation and Model Verification processes to ensure that positive sequence dynamic and EMT models of IBRs accurately reflect real operation behavior of in-service equipment, and improve upon the currently effective MOD-026-1 and MOD-027-1 standards by consolidating them into a single standard. Reliability Standard MOD-026-2 ensures that models, particularly of IBRs, used in operational and planning interconnection studies more accurately represent how these facilities behave during normal periods and disturbance events, and reduce the risk of model-based forecasts being different from real outcomes.

Requirement R1 requires each Transmission Planner and its associated Planning Coordinator to jointly develop dynamic model requirements that are necessary to perform Model Verification and Model Validation and make them readily available to the Generator Owners and Transmission Owners within their area.

- Requirement R1 Part 1.1 requires the Transmission Planner to specify the type of positive sequence models compatible with their planning process.

[21] Under the NERC Rules of Procedure registry criteria. The Generator Owner is defined in Reliability Standards as follows: "The entity that: 1) owns and maintains generating Facility(ies) (Category 1 GO); or 2) owns and maintains non-BES Inverter-Based Resource(s) that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV (Category 2 GO)." *See Notice of Filing of the N. American Elec. Reliability Corp. of Proposed Revisions to the Rules of Procedure to Address Unregistered Inverter Based Resources* (April 5, 2024).

- Requirement R1 Part 1.2 requires the Transmission Planner to document acceptable models, format, and level of detail for generation facilities where EMT models are required and specify the type of EMT models compatible with the Transmission Planner's planning process.

- Requirement R1 Part 1.3 requires the Transmission Planner and their associated Planning Coordinator to document and make available to Generator Owners and Transmission Owners any criteria not listed under Requirement R1, Parts 1.1 and 1.2 that would be used to assess acceptability of the verified and validated dynamic models and accompanying documentation.

- Requirement R1 Part 1.4 requires the Transmission Planner to have guidelines documenting how to resolve unacceptable differences in performance identified under Part 1.3.

Requirement R2 requires Generator Owners and Transmission Owners to provide verified and validated positive sequence dynamic models, associated parameters, and supporting documentation to the Transmission Planner in accordance with the process defined in Requirement R1.

- Requirement R2 Part 2.1 requires that the models submitted reflect the in-service configuration of the facility and physical equipment.

- Requirement R2 Part 2.2 requires verification of site-specific, configurable parameters that can be confirmed by the Generator Owner or Transmission Owner. Parameters such as exciter gains, governor droops, limiter thresholds, and PPC settings significantly impact the dynamic behavior of the facility. This requirement ensures model parameters are consistent with field settings.

- Requirement R2 Part 2.3 requires, at a minimum, Model Validation of the items identified in Parts 2.3.1 and 2.3.2 by using actual behavior from either a stage test, which tests facilities while they are connected to the grid and captures actual operational behavior, or system disturbance.

Attachment 1, Table 1.1, in conjunction with Requirement R2, incorporates synchronous machine aspects of MOD-026-1 Requirement R2. This table, with the requirement, adds more detail and specification about what must be modeled for synchronous generation and synchronous condensers, such as certain limiters and protection systems, including any power oscillation damping controllers, and that the model represents in-service equipment at the facility. Attachment

1, Table 1.2, in conjunction with Requirement R2, incorporates the IBR generation aspects of MOD-026-1 Requirement R2 and MOD-027-1 Requirement R2. This table, with the requirement, adds information that must be provided and additional details on required models for IBR generation. The purpose of this table is to provide clear modeling requirements for dispersed power producing resources outlined in BES Inclusion I4 (IBR facilities), power-based electronics (FACTS devices), and High Voltage Direct Current (HVDC) terminal equipment, so that models represent in-service equipment at each facility.

Attachment 2, Periodicity Table, covers periodicity and certain exemption criteria. Periodicity includes the initial and subsequent Model Verification and Model Validation required time frames for existing and new plants/facilities, and the required time frame for reperforming Model Verification and Model Validation following changes to a plant/facility altering its dynamic response characteristics.

Requirement R3 requires Generator Owners or Transmission Owners to provide verified and validated EMT models to ensure they represent in-service equipment at each IBR facility. This ensures that EMT models for IBR facilities, HVDC equipment, and FACTS devices are developed and used in planning and interconnection analyses.

- Under Requirement R3 Part 3.1 Generator Owners or Transmission Owners are required to submit EMT models that reflect the in-service configuration of the facility and physical equipment.

- Requirement R3 Part 3.2 requires that Generator Owners or Transmission Owners perform Model Verification of site-specific and configurable parameters and ensure EMT model parameters are consistent with field settings.

- Requirement R3 Part 3.3 requires that Generator Owners or Transmission Owners perform Model Validation comparing the behavior of the EMT model to the actual measured behavior during either a stage test, which tests facilities while they are connected to the grid and captures actual operational behavior, or system disturbance.

- Requirement R3 Part 3.4 requires Generator Owners or Transmission Owners to test and have results demonstrating a comparison of the IBR unit response and the IBR unit EMT model response for large signal disturbances.

- Requirement R3 Part 3.5 requires Generator Owners or Transmission Owners to compare the response of the facility positive sequence dynamic model provided in Requirement R2 to the response of the facility EMT model for large signal disturbances as defined by the Transmission Planner.

Requirement R4 requires Generator Owners or Transmission Owners to provide its Transmission Planner with updated model(s) and accompanying documentation within 180 calendar days after making a hardware, software, firmware, control mode, or setting changes to an applicable unit or facility that alters the dynamic response characteristics. This ensures that updated models and accompanying documentation are provided to the Transmission Planner within a reasonable timeframe after any modification to an existing facility that changes the dynamic performance of that facility.

Requirement R5 requires Transmission Planners to review the submitted models and accompanying documentation within 120 calendar days of receiving the models and provide feedback to the Generator Owner or Transmission Owner by either accepting or rejecting the submitted models. This ensures that Transmission Planners determine whether the models and accompanying documentation submitted by the Generator Owners or Transmission Owners meet the acceptable requirements established in Requirement R1.

Requirement R6 requires Generator Owners or Transmission Owners to resubmit models within 120 calendar days after receiving a notification of unacceptability under Requirement R5 or perform a model review within 180 calendar days after receiving a request from its Transmission Planner stating the model or accompanying documentation is deficient. This ensures the Generator Owner or Transmission Owner resolves modeling issues identified by the Transmission Planner, whether as part of the initial model review or sometime thereafter.

Requirement R7 requires Transmission Planners to provide the current models within 90 calendar days of receiving a written request for such data from the Generator Owner or Transmission Owner that owns the facility. This ensures that Generator Owners and Transmission Owners are able to obtain models in instances where facilities change ownership, the model is no longer on file, or there are discrepancies in model records.

Definition of Distributed Energy Resource ("DER"):

A Distributed Energy Resource ("DER") is defined as a generator or energy storage technology connected to a distribution system that is capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including one connected behind the meter of an end-use customer that is supplied from a distribution system.

Definition of Model Validation:

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

Definition of Model Verification:

Model Verification is defined as the process of confirming that model structure and parameter values are representative of the equipment or facility design and settings by reviewing equipment or facility design and settings documentation.

2. *CIP-002-7; CIP-003-10; CIP-004-8; CIP-005-8; CIP-006-7.1; CIP-007-7.1 CIP-008-7.1; CIP-009-7.1; CIP-010 -5; CIP-011-4.1; CIP-013-3 - Virtualization Reliability Standards*[22]

On March 19, 2026, FERC issued Order No. 919 approving 11 Critical Infrastructure Protection ("CIP") Reliability Standards as well as the associated violation risk factors, violation

[22] Proposed Reliability Standards CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, and CIP-011-4.1 all have a .1 designation because they were the subject of an errata that was filed with FERC, *Errata and Supplemental Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection*

severity levels, implementation plans, the retirement of the associated currently effective Reliability Standards, and four new definitions and 18 revised definitions in the *NERC Glossary* of Terms.

The CIP Virtualization Reliability Standards and definitions support reliability by further refining the standards' focus on security through the (1) use of objectives to permit use of a broader variety of security controls, (2) revision of requirements that focused more on compliance documentation, and (3) clarification of issues identified during implementation of prior versions of CIP Reliability Standards.

CIP-002-7 (Cyber Security – BES Cyber System Categorization): Reliability Standard CIP-002-7 requires Responsible Entities to identify and categorize their BES Cyber Systems into low, medium, and high impact based on the assets (e.g., Control Centers, Transmission stations and substations, etc.) these BES Cyber Systems support. Attachment 1 to proposed CIP-002-7 includes criteria that categorize BES Cyber Systems based on the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Revisions to Reliability Standard CIP-002-7 are minor, mostly aligning the standard with updates to the *NERC Glossary*. Additionally, the revised standard incorporates the interpretation regarding "shared BES Cyber System" by clarifying that each "discrete" shared BES Cyber System meets medium impact rating 2.1 in attachment 1 to Reliability Standard CIP-002-7.

CIP-003-10 (Cyber Security – Security Management Controls): Reliability Standard CIP-003-10 requires Responsible Entities to develop cyber security policies to help establish

Reliability Standards, Docket No. RM24-8-000 (May 20, 2025). The errata addressed an error in referencing the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems columns of some of the proposed Reliability Standards. In those proposed Reliability Standards, the first use of the term was incorrectly stated as "Electronic Access Control and Monitoring System (EACMS)" instead of the correct term "Electronic Access Control or Monitoring System (EACMS)". This error has been corrected in the standards being filed herein.

responsibility and accountability through all levels of an organization. The revisions align the requirements with updates to the *NERC Glossary* and apply low impact requirements to virtualized technologies through new proposed terms such as "Shared Cyber Infrastructure" and "Virtual Cyber Asset."

CIP-004-8 (Cyber Security – Personnel & Training): Reliability Standard CIP-004-8 minimizes the risk of individuals inappropriately accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management. The standard includes the following six requirements: (1) Requirement R1 requires a Responsible Entity to implement a documented security awareness process for high and medium impact BES Cyber Systems that reinforces cyber security practices for certain personnel; (2) Requirement R2 requires Responsible Entities to implement a cyber security training program that includes the applicable requirement parts; (3) Requirement R3 requires a documented personnel risk assessment program; (4) Requirement R4 requires a documented access management program(s) that includes the applicable requirement parts; (5) Requirement R5 requires a documented access revocation program(s) that includes the applicable requirement parts; and (6) Requirement R6 requires an access management program(s) to authorize, verify, and revoke provisioned access to BES Cyber System Information that includes the applicable requirement parts.

Reliability Standard CIP-004-8 adds Shared Cyber Infrastructure as an applicable system to help ensure infrastructure that supports virtualized technologies receives appropriate CIP personnel and training protections. In addition, the revisions clarify applicability to medium impact BES Cyber Systems with External Routable Connectivity and those with Interactive Remote Access.

CIP-005-8 (Cyber Security – Electronic Security Perimeter(s)): Reliability Standard CIP-005-8 requires Responsible Entities to develop an Electronic Security Perimeter that only permits certain communications to medium and high impact BES Cyber Systems. The standard includes the three requirements around controlling electronic access to medium and high impact BES Cyber Systems. Requirement R1 requires Responsible Entities to implement one or more documented processes regarding Electronic Security Perimeters. The revised requirement parts incorporate a security objective approach to accommodate more security models.

- Requirement R1, Part 1.2 removes an explicit requirement to use an Electronic Access Point to control communications to applicable systems but replaces it with core security objectives of permitting "only needed routable communications" through the Electronic Security Perimeter and denying all others (excluding time sensitive communications of Protection Systems).
- Requirement R1, Part 1.3 includes a security objective to protect the configurations of Electronic Security Perimeters and Shared Cyber Infrastructure. The requirement part applies to Electronic Access Control or Monitoring Systems that control and create the Electronic Security Perimeter for Applicable Systems in Requirement R1, Part 1.1 and Shared Cyber Infrastructure supporting an Applicable System in Requirement R1, Part 1.1.
- Requirement R1, Part 1.4 adds "SCI supporting an Applicable System in this Part" to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to Virtual Cyber Assets and Shared Cyber Infrastructure; and "where technically feasible" has been replaced with the "per system capability" language.
- Requirement R1, Part 1.5 removes the prescriptive application of protections to the Electronic Access Points and requires malicious routable protocol communications detection entering or leaving the Electronic Security Perimeter.
- Requirement R1, Part 1.6 protects the confidentiality and integrity of the data traversing communication links used to span a single Electronic Security Perimeter between multiple Physical Security Perimeters. It also consolidates the protections of an Electronic Security Perimeter and its components that extend outside of a Physical Security Perimeter within one standard.

Requirement R2 governs protections around remote access management, specifically Interactive Remote Access, used to support and maintain control systems networks. The revisions to Requirement R2 adapt these protections to support virtualized configurations and

clarify issues around defining Interactive Remote Access that arose during implementation of the Version 5 CIP Reliability Standards.

- Requirement R2, Part 2.1 expands safeguards for remote access to Shared Cyber Infrastructure in addition to high and medium impact BES Cyber Systems.
- Requirement R2, Part 2.2 changes the applicability to clarify protections should be applied between the Intermediate System and the remote client rather than between the Intermediate System and the BES Cyber System. In addition, proposed Requirement R2, Part 2.2 changed from a technically specific requirement for encryption to an objective-based requirement to protect the confidentiality and integrity of the Interactive Remote Access session.
- Requirement R2, Part 2.3 clarifies that multi-factor authentication should be applied to the Intermediate System through changes to applicable systems.
- Requirement R2, Parts 2.4 and 2.5 are supply chain protections for vendor remote access sessions. There were only acronym changes and the addition of Shared Cyber Infrastructure to applicability for these requirement parts.
- Requirement R2, Parts 2.6 and 2.7 are new requirement parts focusing on reducing the attack surface between an Intermediate System and the BES Cyber System. Requirement R2, Part 2.6 is intended to prevent a virtualized Intermediate System from sharing central processing units or memory with the BES Cyber System for which it controls access to reduce the risk for a side-channel attack to other Virtual Cyber Assets sharing those resources. Requirement R2, Part 2.7 requires that routable protocol communications between Intermediate Systems and applicable systems in Part 2.1 must be through an Electronic Security Perimeter. This requirement part replaces the language in the currently enforceable definition of Intermediate System that stated an Intermediate System "must not be located inside" the Electronic Security Perimeter.

Requirement R3 applicability was updated to extend the protections for vendor-initiated remote connections to Shared Cyber Infrastructure.

CIP-006-7.1 (Cyber Security – Physical Security of BES Cyber Systems): Reliability Standard CIP-006-7.1 requires a physical security plan to manage physical access to BES Cyber Systems. The revisions apply certain physical protection requirements to virtualization infrastructure where appropriate.

CIP-007-7.1 (Cyber Security – Systems Security Management): Reliability Standard CIP-007-7 specifies technical, operational, and procedural requirements to manage system security

(e.g., malicious code prevention methods, patch management, etc.). The revisions to Reliability Standard CIP-007-7.1 focus on security objectives rather than specific controls for system security management to accommodate virtualized environments. The revised standard also includes Shared Cyber Infrastructure as an applicable system in all requirement parts of CIP-007-7.1. In addition, Reliability Standard CIP-007-7.1 includes a new requirement applicable to Shared Cyber Infrastructure that mitigates vulnerabilities in using the same hardware for different impact categorizations. Finally, the revisions also use "per system capability" instead of "where technically feasible."

Requirement R1 has an updated table name, "System Hardening" (changed from "Ports and Services"), to reflect the security objective of reducing applicable systems' attack surface.

- Requirement R1, Part 1.1 changes its focus from enabling or restricting ports to the broader focus of disabling or preventing unneeded routable protocol network accessibility. Requirement R1, Part 1.1 corrects the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems column of Reliability Standard CIP-007-7.

- Requirement R1, Part 1.3 is a new requirement part applicable to Shared Cyber Infrastructure that supports high or medium impact BES Cyber Systems or their associated Protected Cyber Assets. Requirement R1, Part 1.3 mitigates the risk of exploitation of vulnerabilities of any shared central processing unit resources or memory resources supporting medium or high impact BES Cyber Systems and their associated Protected Cyber Assets by requiring Responsible Entities to prevent the sharing of these resources, excluding storage resources, with Virtual Cyber Assets that are not, or are not associated with, a medium or high impact BES Cyber System.

- Requirements R2, R3, R4, and R5 include minor, conforming changes.

CIP-008-7.1 (Cyber Security – Incident Reporting and Response Planning): Reliability Standard CIP-008-7.1 specifies incident response requirements to mitigate the risk to the reliable operation of the Bulk Electric System resulting from a Cyber Security Incident. The revisions add Shared Cyber Infrastructure to the applicable systems for incident response requirements.

Requirement R1, Part 1.1 corrects the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems column of Reliability Standard CIP-008-7.

CIP-009-7.1 (Cyber Security – Recovery Plans for BES Cyber Systems): Reliability Standard CIP-009-7.1 specifies recovery plan requirements to recover reliability functions of BES Cyber Systems. The revisions add Shared Cyber Infrastructure to the applicable systems where appropriate.

Requirement R1, Part 1.1 corrects the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems column of Reliability Standard CIP-009-7.

CIP-010-5 (Cyber Security – Configuration Change Management and Vulnerability Assessments): Reliability Standard CIP-010-5 governs change management requirements and vulnerability assessment requirements for medium and high impact BES Cyber Systems. The revisions to Reliability Standard CIP-010-5 broaden the change management requirements by incorporating the security objective of controlling the implementation of intended changes to software or settings that could weaken certain cyber security controls rather than only permitting a baseline configuration. Additionally, the revisions add Shared Cyber Infrastructure to applicability where appropriate and replace "where technically feasible" with "per system capability."

The focus of Requirement R1 has changed from documenting the installed software and its open ports on a Cyber Asset or Virtual Cyber Asset at some point post-change, to authorizing the changes that will occur when it does instantiate.

Requirement R2 is modified to adjust the scope of configuration monitoring requirements to conform with revisions to Requirement R1 and support the additional Applicable System (SCI supporting high impact BES Cyber Systems and associated EACMS and PCA).

Requirement R3 requires Responsible Entities to implement a process regarding vulnerability assessments of Applicable Systems.

Requirement R4 requires Responsible Entities to implement a plan to manage Transient Cyber Assets and Removable Media. The revisions within Requirement R4 are mostly conforming and add the term Shared Cyber Infrastructure where appropriate. The revisions within Attachment 1 to Requirement R4 also align language with that in Attachment 1 of proposed CIP-003-10.

CIP-011-4.1 (Cyber Security – Information Protection): Reliability Standard CIP-011-4 specifies information protection requirements to safeguard BES Cyber System Information. The revisions to Reliability Standard CIP-011-4.1 add information protection requirements to Shared Cyber Infrastructure and apply reuse and disposal requirements at a system versus asset level. Proposed Requirement R1 requires Responsible Entities to implement a documented information protection program(s) that includes the applicable requirement parts. Proposed Requirement R2 requires Responsible Entities to implement documented processes regarding BES Cyber Asset reuse and disposal, consistent with the applicable requirement parts.

Requirement R1, Part 1.1 corrects the Glossary term "Electronic Access Control or Monitoring System (EACMS)" in the Applicable Systems column of Reliability Standard CIP-011-4.

CIP-013-3 (Cyber Security – Supply Chain Risk Management): Reliability Standard CIP-013-3 requires Responsible Entities to consider and address cyber security risks from vendor products or services during planning for the procurement of BES Cyber Systems as well as

Electronic Access Control or Monitoring Systems and Physical Access Control Systems. Reliability Standard CIP-013-3 includes three requirements: (1) Requirement R1 requires a Responsible Entity to develop documented supply chain cyber security risk management plan(s) and includes requirement parts detailing the processes to include in the plan; (2) Requirement R2 requires Responsible Entities to implement the plan(s); and (3) Requirement R3 requires review and CIP Senior Manager, or delegate, approval of the plan(s) at least once every 15 calendar months. The revisions extend these supply chain risk management requirements to Shared Cyber Infrastructure.

There were several other modifications throughout the CIP Reliability Standards that are clarifying or conforming changes. Additionally, there are several revisions that are administrative in nature, such as use of acronyms, streamlining the Violation Severity Levels, removing functional entities no longer subject to Reliability Standards, and removing the non-enforceable Background and Guidelines and Technical Basis sections to separate technical rationale documents.

Definitions of newly defined terms

Cyber System:

Cyber System is defined as: One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Management Interface:

Management Interface is defined as: An administrative interface that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an Electronic Access Point.

Shared Cyber Infrastructure ("SCI"):

Shared Cyber Infrastructure is defined as: One or more programmable electronic devices, including the software that shares the devices' resources, that:

- Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

Virtual Cyber Asset:

Virtual Cyber Asset is defined as: A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include:

- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file-based images that contain operating systems or firmware; or
- SCI or Cyber Assets that host VCAs.

Application containers are considered software of VCAs or Cyber Assets.

Definitions of Revised Terms

BES Cyber Asset:

BES Cyber Asset is defined as: A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the

Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

BES Cyber System Information ("BCSI"):

BES Cyber System Information is defined as: Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BCSI does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.

Critical Infrastructure Protection ("CIP") Senior Manager:

CIP Senior Manager is defined as: A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Cyber Security Standards.

Cyber Assets:

Cyber Assets is defined as: Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCA) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Cyber Security Incident:

Cyber Security Incident is defined as: A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BCS.

Electronic Access Control or Monitoring Systems ("EACMS"):

EACMS is defined as: Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.

Electronic Access Point:

Electronic Access Point is defined as: An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.

External Routable Connectivity:

External Routable Connectivity is defined as: The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Electronic Security Perimeter:

Electronic Security Perimeter is defined as: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.

Interactive Remote Access:

Interactive Remote Access is defined as: User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or
- System-to-system process communications.

Intermediate System:

Intermediate System is defined as: One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Physical Access Control Systems:

Physical Access Control Systems is defined as: Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter:

Physical Security Perimeter is defined as: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Protected Cyber Asset:

Protected Cyber Asset is defined as: One or more Cyber Assets or Virtual Cyber Assets (VCA) that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or
- Share CPU resources or memory resources with any part of the BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS;

Excluding Transient Cyber Assets.

Removable Media:

Removable Media is defined as: Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.

Reportable Cyber Security Incident:

Reportable Cyber Security Incident is defined as: A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BCS;
- An Electronic Access Control or Monitoring System of a high or medium impact BCS; or
- Shared Cyber Infrastructure supporting a BCS.

Transient Cyber Asset:

Transient Cyber Asset is defined as a Cyber Asset or Virtual Cyber Asset (VCA) that is:

1. Capable of transmitting or transferring executable code,
2. Not included in a BCS,
3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS, and
4. Connected for 30 consecutive calendar days or less:
   - On a network within an Electronic Security Perimeter containing high or medium impact BCS; or
   - Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:

- BES Cyber Asset;
- Shared Cyber Infrastructure; or
- PCA associated with high or medium impact BCS.

Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

BES Cyber System:

The NERC Glossary update includes BCS as the acronym for BES Cyber System. No changes were made to the definition.

3. *CIP-003-11 (Cyber Security - Security Management Controls):*

On March 19, 2026, FERC issued Order No. 918 approving Reliability Standard CIP-003-11 (Cyber Security – Security Management Controls) as well as the associated violation risk factors and violation severity levels, implementation plan, and the retirement of the currently effective version of the Reliability Standard upon the effective date of Reliability Standard CIP-003-11. Reliability Standard CIP-003-11 enhances reliability by mitigating the risk posed by a coordinated attack utilizing distributed low impact BES Cyber Systems. The standard adds controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to or between assets containing low impact BES Cyber Systems with External Routable Connectivity.

Revisions to Reliability Standard CIP-003-11 were layered on top of virtualization revisions to Reliability Standard CIP-003-10, which had been approved by the NERC Board of Trustees but was pending regulatory approval at the time Reliability Standard CIP-003-11 was completed and approved by the NERC Board of Trustees and filed with FERC and the applicable governmental authorities. Reliability Standard CIP-003-10 was approved by FERC in Order No. 919, which was issued concurrently with Order No. 918 approving CIP-003-11. As approved by

FERC, CIP-003-10 will become effective on July 1, 2028 and will then be retired and superseded by Reliability Standard CIP-003-11 on July 1, 2029.

The title, purpose, and applicability of Reliability Standard CIP-003-11 remain unchanged from CIP-003-10. The only new change that has been made to the requirements is the removal of Requirement R1 Part 1.2.6 Vendor electronic remote access security controls. This change reflects the deletion of Attachment 1 Section 6, Vendor Electronic Remote Access and Security Controls, which was combined into Attachment 1 Section 3, Electronic Access Controls.

Reliability Standard CIP-003-11 revises Attachment 1 of the standard by merging Section 3 (Electronic Access Controls) and Section 6 (Vendor Electronic Remote Access and Security Controls) into a new revised Section 3 in order to have a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). While merging Sections 3 and 6, the drafting team made conforming changes to certain language. Specifically, the proposed standard would use the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". This change reflects that a "control" may include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the proposed standard would remove the word "remote" from the phrase "electronic remote access" as the section would now include all electronic access as described in Attachment 1 Section 3 Part 3.1, (i), (ii), and (iii).

Attachment 1 Section 3.1.2 would expand the scope of Reliability Standard CIP-003 to include all communications, rather than only vendor specific communications. Proposed Section 3.1.2 would require that entities implement controls to detect known or suspected inbound and outbound malicious communications between low impact BES Cyber Systems and a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems. These revisions would

enable entities to mitigate the risk posed by malicious communications to or from low impact BES Cyber Systems, while allowing entities flexibility as to where the control is implemented based on their architecture.

Attachment 1 Section 3.1.3 would mitigate the risk of unauthenticated access to networks on which low impact BES Cyber Systems reside. Specifically, the proposed revisions would require entities to implement controls to authenticate users prior to permitting (allowing, establishing, gaining) access to networks containing low impact BES Cyber Systems, or Shared Cyber Infrastructure ("SCI") that supports a low impact BES Cyber System.

Attachment 1 Section 3.1.4 would require Responsible Entities to protect the user authentication information (e.g., username, password, multi-factor authentication information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3.53 This protection would mitigate the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text.

Section 3.1.5 would preserve the language used in proposed Reliability Standard CIP-003-10, Section 6.1 and merge it into revised Section 3. This would require Responsible Entities to implement one or more method(s) for determining vendor electronic access, where permitted, to their low impact BES Cyber Systems, thus increasing an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6 would preserve the language used in proposed Reliability Standard CIP-003-10, Section 6.2. This would require Responsible Entities to implement one or more method(s) for disabling vendor electronic remote access, where permitted, for any basis the entity may choose.

This would prevent security events and propagation of potential malicious communications that may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems.

The standard revises Attachment 2 by merging Section 6 into Section 3 to conform with changes in Attachment 1. The proposed revisions include providing examples of compliance related activities.

4. CIP-002-8 (Cyber Security-BES Cyber System Categorization)

On March 19, 2026, FERC issued a letter order approving Reliability Standard CIP-002-8, the associated violation risk factors and violation severity levels, the implementation plan, the definition of Control Center for use in the *NERC Glossary*, as well as the retirement of Reliability Standard CIP-002-7 prior to the effective date of Reliability Standard CIP-002-8.

Revisions to Reliability Standard CIP-002-8 were layered on top of the revisions contained in Reliability Standard CIP-002-7, which had been approved by the NERC Board of Trustees but was pending was FERC approval at the time of filing. Thus, the revisions that were first proposed in CIP-002-7 were carried forward and included in Reliability Standard CIP-002-8 and accounted for in the CIP-002-8 Implementation Plan. As a result, CIP-002-8 was specifically designed to replace CIP-002-7 if they were approved by FERC on or near the same date. FERC approved both CIP-002-7 and CIP-002-8 in concurrently issued orders on the same date. As a result, CIP-002-8 will replace CIP-002-7 on the proposed effective date.

Reliability Standard CIP-002-8 enhances reliability by revising Criterion 2.12 of Attachment 1 to the standard. Specifically, the revisions to Criterion 2.12 of Attachment 1 clarify the "bright line" criteria for Transmission Owners and Transmission Operators to categorize their BES Cyber Systems based on the impact to their associated Facilities, systems,

and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the BES. The revisions address the categorization of Transmission Owner Control Centers with the capability to control transmission Facilities. In order to assess the appropriate impact level of the BES Cyber Systems associated with a Control Center, Attachment 1 Criterion 2.12 assigns a weight value to the Transmission Lines that a Control Center monitors and controls, as portrayed in the table included in the proposed revisions to Criterion 2.12. The total aggregate weighted value is used to account for the impact on the BES. As revised, Criterion 2.12 uses a total aggregate weighted value of 6,000, which was derived based on an entity with no single station or substation that meets Criterion 2.5, but has the capability or authority to control BES Transmission Lines with the equivalent weight of two stations or substations whose BES Cyber Systems would be classified as medium impact per Criterion 2.5. This was derived from the "two or more locations" criterion documented in the proposed Control Center definition.

For consistency with the existing Attachment 1 criteria, the weighted values for the various voltage classes of BES Transmission Lines were selected to align with the existing approved values in Criterion 2.5.

In addition, the revisions clarify the "perform the functional obligations of" language throughout Attachment 1 by instead referring to the reliability tasks performed by those same Registered Entities or, in the case of the Transmission Operator and the Transmission Owner, reference to the Control Center definition with respect to "reliability tasks" or "capability to control transmission Facilities", as appropriate.

An exclusion clause was also added to Criterion 2.12, in recognition that some Control Centers whose aggregate weighted value of lines exceeds 6,000 may have a negligible impact

on the reliability of the BES if BES Cyber Systems were compromised. The exclusion clause allows Responsible Entities to appropriately categorize their BES Cyber Systems at Control Centers at a level that is commensurate with the associated risk for local systems having limited flow-through or generation export, and are primarily designed to serve load. The exclusion clause applies to Transmission Operators and Transmission Owners where the initial calculated aggregate weighted value is less than 12,000. In such cases, the Transmission Operator/Transmission Owner may calculate a revised aggregate weighted value that excludes those BES Transmission Lines that are contained in a single group of contiguous Elements operated at or greater than 69 kV but less than 300 kV, as defined by the Responsible Entity. The hourly integrated gross export from the group of contiguous Elements is not allowed to exceed 75 MWh during the preceding 12 calendar months during non-Energy Emergency Alert conditions. Gross exports from the group of contiguous Elements during an Energy Emergency Alert condition that exceed 75 MWh are allowed to enable the Responsible Entity to provide support to neighboring entities during Energy Emergency Alert conditions without any compliance impact.

Definition of Control Center:

NERC proposes a revised definition of the term Control Center for inclusion in the *NERC Glossary* to address ambiguities found during a field test that many Transmission Owners struggled with how to interpret the Control Center definition in CIP-002-5.1a because it does not specifically identify Transmission Owners, even though a Transmission Owner may have a Control Center through its ability to monitor and control the BES in real-time to perform the reliability tasks of a Transmission Operator. Thus, the definition of Control Center is revised as follows:

> One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
>
> Or
>
> One or more facilities of a Transmission Owner that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers, and excluding field Cyber Assets used for telemetry.

5. *BAL-007-1.1 Errata (Near-Term Energy Reliability Assessments)*

On March 26, 2026, FERC issued a letter order approving the errata to Reliability Standard BAL-007-1. FERC approved Reliability Standard BAL-007-1 on February 26, 2025. The errata changes capitalize the first letter of the word "term" in the defined term "Near-Term Energy Reliability Assessment." The term is used in the standard title, Requirement R6, and Measure R6 of Reliability Standard BAL-007-1.

D. Description of Proposed NERC Glossary Definitions, Second Quarter 2024

NERC submits for approval the definitions of terms related to the calculation of Reporting Area Control Error or Reporting ACE approved by FERC in the second quarter of 2024. NERC discovered that these definitions were inadvertently not submitted with a standalone application for approval in the quarter following FERC approval in 2024; however, they have been provided to Nova Scotia with each subsequent version of the NERC Glossary of Terms. As provided below, on April 29, 2024, FERC issued an order approving the Reporting ACE definitions for inclusion in the *Glossary of Terms used in NERC Reliability Standards* **(Exhibit C)**. In support of this request for approval, NERC submits the following information: a table listing the United States effective date of each definition applicable to Nova Scotia that was approved by FERC in the

second quarter of 2024 **(Exhibit A-4)**; an informational summary of the definitions applicable to Nova Scotia that were approved by FERC in the second quarter of 2024, including the date that NERC filed the definitions with FERC and the date that FERC approved the definitions **(Exhibit A-5)**; and the revised Reporting Ace Definitions for inclusion in the *NERC Glossary* that were approved by FERC during the second quarter of 2024 **(Exhibit A-6)**.

6. Reporting ACE Definitions

NERC submits for approval two new, thirty modified, and four retired definitions of terms related to the calculation of Reporting Area Control Error or Reporting ACE, for inclusion in the Glossary of Terms used in NERC Reliability Standards ("Reporting ACE Glossary Terms"). The Glossary Terms define, or are related to, the components of Reporting Area Control Error, or Reporting ACE. Reporting ACE is one of the most important single measurements available to indicate the current state of the responsible entity's contribution to Interconnection reliability.

These terms include the following:

- ***New Glossary Terms***: ACE Diversity Interchange, Inadvertent Interchange Management (IIM);
- ***Revised Glossary Terms***: Actual Net Interchange (NIA); Area Control Error (ACE); Automatic Generation Control (AGC); Automatic Time Error Correction (ATEC); Balancing Authority Area (BAA); Balancing Contingency Event (BCE); Control Performance Standard (CPS); Disturbance; Dynamic Interchange Schedule or Dynamic Schedule; Frequency Bias Setting (FBS); Frequency Error; Implemented Interchange; Inadvertent Interchange; Interchange Meter Error (IME); Operating Reserve – Spinning; Operating Reserve – Supplemental; Overlap Regulation Service; Pseudo-Tie; Ramp Rate or Ramp; Regulation Service; Reportable Balancing Contingency Event (RBCE); Reporting Area Control Error (Reporting ACE); Reserve Sharing Group (RSG); Reserve Sharing Group Reporting ACE; Scheduled Frequency; Scheduled Net Interchange (NIS); Supplemental Regulation Service; Tie Line Bias (TLB); Time Error (TE); Time Error Correction (TEC);
- *Retired Glossary Terms*: Disturbance Control Standard; Net Interchange Schedule; Net Scheduled Interchange; Reportable Disturbance

The project to address Reporting ACE was the result of the NERC Reliability and Security Technical Committee Resources Subcommittee's identification of a large amount of accumulated time error in the Eastern Interconnection because the Reporting ACE definition only referred to Automatic Time Error Correction as a component only in the Western Interconnection. Thus, the revised definition has been modified to accommodate any Interconnection that has an approved automatic time error correction methodology or other process to control inadvertent accumulation. The Reporting ACE Glossary Terms, including the revised definition of Reporting ACE, allow for any Interconnection to implement an approved automatic time error correction methodology or other process to control inadvertent accumulation. The Reporting ACE Glossary Terms improve clarity regarding the components that make up the Area Control Error used for reporting. Further, the revised definition of Reporting ACE, with the new incorporated definition of Inadvertent Interchange Management, resolves a conflict in the current definition of Reporting ACE with the Western Interconnection's Automatic Time Error Correction process.

The revised definition of Reporting ACE, the new terms for inclusion in the revised definition of Reporting ACE, and refinements and corrections to definitions of the components of Reporting ACE are below:

Definition of Reporting Area Control Error ("Reporting ACE"):

Reporting ACE is defined as: The scan rate values of a Balancing Authority Area's Area Control Error (ACE) measured in MW, which includes the error in scheduled interchange adjusted for Frequency Bias obligation, known meter error, and inadvertent management. Reporting ACE is calculated as follows:

Reporting ACE = $(NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME} + I_{IM}$ Where:

- NI_A = Actual Net Interchange.
- NI_S = Scheduled Net Interchange.

- B = Frequency Bias Setting.
- F_A = Actual Frequency.
- F_S = Scheduled Frequency.
- I_{ME} = Interchange Meter Error.
- I_{IM} = Inadvertent Interchange Management. (Term is expressed if a regional procedure exists, otherwise is null and is not included in the Balancing Authority's Reporting ACE.)

All NERC Interconnections operate using the principles of Tie Line Bias (TLB) control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE that is(are) implemented for all BAAs in an Interconnection and is(are) consistent with the following four principles of Tie Line Bias control will provide a valid alternative to this Reporting ACE equation:

1. Each individual portion of the Interconnection is included in exactly one BAA so that the sum of all BAAs' generation, Load, and losses is the same as total Interconnection generation, Load, and losses;

2. The algebraic sum of all BAAs' Scheduled Net Interchange is equal to zero at all times and the sum of all BAAs' Actual Net Interchange values is equal to zero at all times. This includes effects of ACE Diversity Interchange (ADI) implementations;

3. The use of a common Scheduled Frequency for all BAAs at all times; and,

4. Excludes metering or computational errors. (The inclusion and use of the IME term corrects for known metering or computational errors.)

Definition of Area Control Error ("ACE"):

Area Control Error is defined as: The instantaneous difference between an entity's Actual Net Interchange (NI_A) and Scheduled Net Interchange (NI_S), taking into account the effects of Frequency Bias, of correction for meter error, and of Inadvertent Interchange Management (I_{IM}) if operating in the I_{IM} mode. For Compliance usage, refer to the term Reporting ACE.

Definitions of Components of Reporting ACE:

The revisions to terms that comprise the Reporting ACE calculation correct capitalization, grammar, and reflect current terminology and practice, as described below:

- **Actual Net Interchange (NI_A)**: revised to correct capitalization of defined terms as follows: The algebraic sum of actual megawatt transfers across all Tie Lines, including Pseudo-Ties, to and from all Adjacent Balancing Authority Areas within the same Interconnection. Actual megawatt transfers on asynchronous DC tie lines

that are directly connected to another Interconnection are excluded from Actual Net Interchange.

- **Scheduled Net Interchange (NI_S)**: adds acronym to definition.
- **Frequency Bias Setting (FBS)**: revised to indicate that this value must be a negative number, eliminates language regarding practice, and updated to reflect current terminology, as follows: A negative number either fixed or variable, expressed in MW/0.1 Hz, included in a Balancing Authority's Reporting ACE to account for the Balancing Authority's Frequency Response to the Interconnection Frequency Error, and discourage response withdrawal through secondary control systems.
- **Scheduled Frequency (F_S):** adds resolution to the term, as Time Error corrections are normally performed in +/- .02 Hz increments, and capitalizes defined terms, as follows: 60.00 Hertz, except during a Time Error Correction.
- **Interchange Meter Error (I_{ME})**: eliminates the word "calculation" for consistency, as follows: A term used in Reporting ACE to compensate for data or equipment errors affecting any other components of Reporting ACE.
- **Inadvertent Interchange Management (I_{IM}) (*new definition*)**: defined as, "a term used in Reporting ACE to allow for management of Inadvertent Interchange and correction of Time Error. The I_{IM} value is not used for unilateral paybacks and is null unless there is a regional procedure in place to coordinate an inadvertent control methodology for an Interconnection."
- **Automatic Time Error Correction (ATEC)**: revised to advance a more accurate calculation of Automatic Time Error Correction and provides for increased clarity and consistency. Revisions include adding an islanding term, "BAIsland", to reflect that a Balancing Authority that has lost synchronism with the remainder of the interconnection cannot have an impact on the interconnection's Time Error; amending the method of allocating Primary Inadvertent Interchange to use actual Bias settings to reflect each Balancing Authority's share of Time Error impact more accurately; and making several conforming and correction changes throughout.
- **ACE Diversity Interchange (ADI) (*new definition*)**: defined as, "a frequency neutral exchange program where multiple participating Balancing Authorities utilize it to achieve reductions in their generation control and Reporting ACE through offsets to either Actual Net Interchange or Scheduled Net Interchange ACE components to create an ACE value closer to zero for each participant."

Definitions of Reporting ACE Related Terms:

The revisions to other *NERC Glossary* terms related to the calculation of Reporting ACE, defined terms used directly or indirectly in the definition of Reporting ACE, or terms that refer to ACE or Reporting ACE are summarized below:

- **Automatic Generation Control (AGC)**: minor grammatical corrections (errata) as follows: "A process designed and used to adjust a Balancing Authority Area's ~~'~~ Demand and resources to help maintain the Reporting ACE in that ~~of a~~ Balancing Authority Area within the bounds required by applicable NERC Reliability Standards."
- **Balancing Authority Area (BAA)**: adds acronym.
- **Balancing Contingency Event (BCE)**: adds acronym, revises internal references to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology.
- **Control Performance Standard (CPS)**: replaces current definition, which refers to a specific standard ("The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period"), with a more generally applicable definition that refers to the methodology. ("Methodology of controlling Reporting ACE relative to Frequency Error, expressed as a moving average subject to a limit. It is used as an indicator of sufficient secondary AGC control to maintain energy balance and Scheduled Frequency.")
- **Disturbance**: revises internal references to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology.
- **Dynamic Interchange Schedule or Dynamic Schedule**: revises internal reference to "control ACE equations" to "Reporting ACE" for consistency and to reflect current terminology, and eliminates a parenthetical ("or alternate control processes") that has no known application.
- **Frequency Error**: corrects grammar and capitalization of defined terms.
- **Inadvertent Interchange**: updates to reflect current *NERC Glossary* terms and correct acronyms for Actual Net Interchange and Scheduled Net Interchange (NI_A – NIs).
- **Implemented Interchange**: revises internal reference to the term "Area Control Error equation" to "Reporting ACE" for consistency and to reflect current terminology.
- **Operating Reserve – Spinning**: corrects capitalization of the phrase "Recovery Period" which is not a *NERC Glossary* term.
- **Operating Reserve – Supplemental**: corrects capitalization of the phrase "Recovery Period," which is not a *NERC Glossary* term.
- **Overlap Regulation Service**: updated to reflect correct use of defined terms and revise internal reference to "ACE" to "Reporting ACE" for consistency.
- **Pseudo-Tie**: revises internal reference to "Reporting ACE equation" to "Reporting ACE" for consistency, and eliminates a parenthetical ("or alternate control processes") that has no known application.
- **Ramp Rate or Ramp**: capitalizes the term "Interchange Schedule" within the definition.

- **Regulation Service**: revises internal reference to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology, and replaced the phrase "Regulation Service" in definition with "corrective response" to avoid using the defined term within the definition.
- **Reportable Balancing Contingency Event (RBCE)**: revises internal reference to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology, adds acronym for the phrase "Most Severe Single Contingency (MSSC)," and moves the provision regarding reducing the 80% threshold from subpart (ii) to subpart (i) for readability.
- **Reserve Sharing Group Reporting ACE**: revises internal reference to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology.
- **Supplemental Regulation Service**: revises internal reference to the term "ACE" to "Reporting ACE" for consistency and to reflect current terminology, and capitalizes defined term "Regulation Service."
- **Tie Line Bias (TLB)**: capitalizes defined term "Frequency Error" within definition.
- **Time Error (TE)**: adds acronym to definition and makes minor grammatical change to definition.
- **Time Error Correction (TEC)**: adds the word "manual" before "offset" to indicate that this process is not implemented automatically; minor grammatical and wording changes; capitalizes term "Scheduled Frequency."

Definition of Reserve Sharing Group:

Reserve Sharing Group is modestly revised as follows:

> A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply O~~o~~perating R~~r~~eserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in more quickly~~er~~ (e.g., between zero and ten minutes) then, for the purposes of recovery from a Reportable Balancing Contingency Event~~disturbance control performance~~, the areas become a Reserve Sharing Group.

Retired Terms:

NERC proposes to retire four "version zero" terms from the NERC Glossary, initially approved by FERC in 2007, as these definitions are no longer used, or will no longer be needed

following the effective date of the definitions for the new and revised NERC Glossary terms discussed earlier in this filing. Retirement of these terms is appropriate due to the discontinuation of their use and would provide clarity to entities regarding terms that are used in currently enforceable NERC Reliability Standards or Glossary terms. Thus, NERC seeks approval to retire the following terms:

- **Disturbance Control Standard (DCS)**: defined as, "The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return its Area Control Error to within a specified range."
- **Net Interchange Schedule**: defined as, "The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority."
- **Net Scheduled Interchange**: defined as, "The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time."
- **Reportable Disturbance**: defined as, "Any event that causes ACE change greater than or equal to 80% of a Balancing Authority's or reserve sharing group's most severe contingency. The definition of a reportable disturbance is specified by each Regional Reliability Organization. This definition may not be retroactively adjusted in response to observed performance."

III. CONCLUSION

NERC respectfully requests that NSEB approve the Reliability Standards and Definitions as specified herein.

Respectfully submitted,

/s/ *Sarah P. Crawford*

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Senior Counsel
Marisa Hecht
Senior Counsel
Alain Rigaud
Associate Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net
sarah.crawford@nerc.net
marisa.hecht@nerc.net
alain.rigaud@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: May 28, 2026

Exhibit A-1

Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026

Exhibit A-1:
Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026

Reliability Standard	Effective Date
Modeling, Data, and Analysis (MOD)	
MOD-032-2*	4/1/2028
MOD-033-3	4/1/2026
MOD-026-2	4/1/2026
Interconnection Reliability Operations and Coordination (IRO)	
IRO-010-6*	4/1/2029
Transmission Operations (TOP)	
TOP-003-8*	4/1/2029
Critical Infrastructure Protection (CIP)	
CIP-002-7**	7/1/2028
CIP-003-10*	7/1/2028
CIP-004-8*	7/1/2028
CIP-005-8*	7/1/2028
CIP-006-7.1*	7/1/2028
CIP-007-7.1*	7/1/2028
CIP-008-7.1*	7/1/2028
CIP-009-7.1*	7/1/2028
CIP-010-5*	7/1/2028
CIP-011-4.1*	7/1/2028
CIP-013-3*	7/1/2028
CIP-002-8* **	7/1/2028
CIP-003-11*	
Resource and Demand Balancing (BAL)	
BAL-007-1*	4/1/2027

*At the time of this filing, the standards marked with an asterisk are not yet effective but have been approved by FERC and have a future mandatory effective date.

** On March 19, 2026, FERC issued orders that approve revisions to two versions of Reliability Standard CIP-002, CIP-002-7 and CIP-002-8. The revisions that were first proposed in CIP-002-7 were carried forward and included in Reliability Standard CIP-002-8 and accounted for in the CIP-002-8 Implementation Plan. As a result, CIP-002-8 was specifically designed to replace CIP-002-7 in the event that they were approved by FERC on or near the same date.

Exhibit A-2

Informational Summary of Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026

Exhibit A-2:
Informational Summary of Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2026

Reliability Standard MOD-032-2	
Purpose	To establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system.
Applicability	Functional Entities: • Balancing Authority • Distribution Provider • Generator Owner • Planning Authority and Planning Coordinator (hereafter collectively referred to as "Planning Coordinator") • Resource Planner • Transmission Owner • Transmission Planner • Transmission Service Provider
Requirements	Reliability Standard MOD-032-2 includes four requirements.
Date of Petition and FERC Order	Petition filed on November 4, 2025, for approval of proposed Reliability Standard MOD-032-2 with FERC in Docket No. RD26-1-000. FERC approved the Reliability Standard on February 19, 2026.

Reliability Standard IRO-010-6	
Purpose	To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring each Reliability Coordinator has the data and information it needs to plan, monitor and assess the operation of its Reliability Coordinator Area.
Applicability	Functional Entities: • Reliability Coordinator • Balancing Authority • Generator Owner • Generator Operator • Transmission Operator • Transmission Owner • Distribution Provider
Requirements	Reliability Standard IRO-010-6 includes three requirements.
Date of Petition and FERC Order	Petition filed on November 4, 2025, for approval of proposed Reliability Standard IRO-010-6 with FERC in Docket No. RD26-1-000. FERC approved the Reliability Standard on February 19, 2026.

Reliability Standard TOP-003-8	
Purpose	To ensure that each Transmission Operator and Balancing Authority has the data and information it needs to plan, monitor, and assess the operation of its Transmission Operator Area or Balancing Authority Area.
Applicability	Functional Entities: • Transmission Operator • Balancing Authority • Generator Owner • Generator Operator • Transmission Owner • Distribution Provider
Requirements	Reliability Standard TOP-033-8 includes four requirements.
Date of Petition and FERC Order	Petition filed on November 4, 2025, for approval of proposed Reliability Standard TOP-033-8 with FERC in Docket No. RD26-1-000. FERC approved the Reliability Standard on February 19, 2026.

Reliability Standard MOD-033-3	
Purpose	To establish a process for system model validation to facilitate achieving and maintaining model accuracy.
Applicability	Functional Entities: • Planning Coordinator • Reliability Coordinator • Transmission Coordinator
Requirements	Reliability Standard MOD-033-3 includes two requirements.
Date of Petition and FERC Order	Petition filed on November 4, 2025, for approval of proposed Reliability Standard MOD-033-3 with FERC in Docket No. RD26-2-000. FERC approved the Reliability Standard on February 19, 2026.

Reliability Standard MOD-026-2	
Purpose	To verify and validate that the dynamic models and associated parameters used to assess Bulk Electric System (BES) reliability represent the inservice equipment of Bulk Power System (BPS) facilities including generating facilities, transmission connected dynamic reactive resources, and high-voltage direct current (HVDC) systems.
Applicability	Functional Entities: • Generator Owner • Planning Coordinator • Transmission Owner • Transmission Planner
Requirements	Reliability Standard MOD-026-2 includes seven requirements.
Date of Petition and FERC Order	Petition filed on November 4, 2025, for approval of proposed Reliability Standard MOD-026-2 with FERC in Docket No. RD26-3-000. FERC approved the Reliability Standard on February 19, 2026.

Reliability Standard CIP-002-8	
Purpose	To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Balancing Authority • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-002-8 includes two requirements.
Date of Petition and FERC Order	Petition filed on December 20, 2024, for approval of proposed Reliability Standard CIP-002-8 with FERC in Docket No. RD25-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-003-11	
Purpose	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-003-10 includes four requirements.
Date of Petition and FERC Order	Petition filed on December 20, 2024, for approval of proposed Reliability Standard CIP-003-11 with FERC in Docket No. RM25-8-000. FERC approved the Reliability Standard on March 19, 2026.

Virtualization Reliability Standards

Reliability Standard CIP-002-7	
Purpose	To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-002-7 includes two requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-002-7 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-003-10	
Purpose	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common ▪ control system owned by the Responsible Entity, ▪ without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-003-10 includes four requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-003-10 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May,20, 2025 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-004-8	
Purpose	To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-004-8 includes six requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-004-8 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-005-8	
Purpose	To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-005-8 includes three requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-005-8 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-006-7.1	
Purpose	To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-006-7.1 includes three requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-006-7.1 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May 20, 2025, with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-007-7.1	
Purpose	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-007-7.1 includes five requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-007-7.1 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May 20, 2025, with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-008-7.1	
Purpose	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-008-7.1 includes four requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-008-7.1 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May 20, 2025, with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-009-7.1	
Purpose	To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-009-7.1 includes three requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-009-7.1 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May 20, 2025, with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-010-5	
Purpose	To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-010-5 includes four requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-010-5 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-011-4.1	
Purpose	To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-011-4.1 includes two requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-011-4.1 with FERC in Docket No. RM24-8-000. The Errata and Supplemental Petition was filed on May 20, 2025, with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard CIP-013-3	
Purpose	To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).
Applicability	Functional Entities: • Balancing Authority • Distribution Provider that owns one of the following Facilities, systems, and equipment for protection or restoration of the BES: o Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o 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. o 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. • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner
Requirements	Reliability Standard CIP-013-3 includes three requirements.
Date of Petition and FERC Order	Petition filed on July 10, 2024, for approval of proposed Reliability Standard CIP-013-3 with FERC in Docket No. RM24-8-000. FERC approved the Reliability Standard on March 19, 2026.

Reliability Standard BAL-007-1.1	
Purpose	To assess, report, and plan to address forecasted Energy Emergencies in the near-term time horizon.
Applicability	Functional Entities: • Balancing Authority
Requirements	Reliability Standard BAL-007-1.1 includes six requirements.
Date of Petition and FERC Order	Petition filed on 23, 2026, for approval of proposed Reliability Standard BAL-007-1.1 with FERC in Docket No. RD26-4-000. FERC approved the Reliability Standard on March 26, 2026.

Exhibit A-3

Reliability Standards Filed for Approval

Reliability Standard MOD-032-2

A. Introduction

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

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

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

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider

   4.1.3 Generator Owner

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

   4.1.5 Resource Planner

   4.1.6 Transmission Owner

   4.1.7 Transmission Planner

   4.1.8 Transmission Service Provider

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

B. Requirements and Measures

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

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

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

1.2.1. Data format;

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

1.2.3. Case types or scenarios to be modeled; and

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

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

1.4. Specifications of the following items for dynamic model submissions:

1.4.1. Required submission of:

- standard library models incorporated within the software(s) utilized to create the Interconnection-wide case(s);
- user-defined models; or
- both standard library models and user-defined models.

1.4.2. Where user-defined models are accepted, usability requirements for any submitted user-defined models including, at a minimum, requirements to provide model documentation and instructions for model set up and use.

1.4.2.1. Each Planning Coordinator and Transmission Planner shall provide their user-defined model requirements within 90 calendar days of receiving a written request for such data from other Planning Coordinators and Transmission Planners within the Interconnection.

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

R2. Each Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, and Transmission Service Provider shall provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures

developed by its Planning Coordinator and Transmission Planner in Requirement R1. For data that has not changed since the last submission, a written confirmation that the data has not changed is sufficient. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. If a functional entity is required to provide data for one or more of the following and is unable to gather such data, the functional entity shall provide an estimate of the data, an explanation of the limitations of the estimated data, and the method used for estimation;

- Aggregate DER data; or
- Data for an IBR that is not a DER and does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.

2.2. If a functional entity is required to provide dynamic models, the functional entity shall provide the models accepted by the Transmission Planner under MOD-026, where such models are available.

2.3. If a functional entity provides a model that is included on the Unacceptable Models List maintained by the ERO in accordance with the process described in the MOD-032 Supporting Document, the functional entity shall also provide a technical rationale justifying the use of that model.

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

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

3.1. Provide either updated data or an explanation with a technical basis for maintaining the current data that is responsive to the technical concern.

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

M3. Each functional entity identified in Requirement R3 that has received written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2 shall provide evidence, such as email records or postal receipts showing recipient and date, that it has provided either updated data or an explanation with a technical basis for maintaining the current data to its Planning Coordinator or Transmission Planner within 90 calendar days of receipt (or within the longer time period agreed upon by the notifying

Planning Coordinator or Transmission Planner), or a statement that it has not received written notification regarding technical concerns with the data submitted.

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

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

C. Compliance

1. **Compliance Monitoring Process**

   1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

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

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

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

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

3. **Potential Noncompliance (PNC) Abeyance Period:**
Potential Noncompliance (PNC) Abeyance Period: For a period of two years following the phased-in compliance date of Reliability Standard MOD-032-2 Requirement R2 under the associated implementation plan, the CEA will not pursue an action under Sections 4A.0 or 5.0 of Appendix 4C to the Rules of Procedure for a failure to comply with Reliability Standard MOD-032-2 Requirement R2 Part 2.1 with respect to the provision of estimated aggregate DER data or estimated data for an IBR that is not a DER and does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes against any entity acting in good faith to comply with the standard in accordance with the relevant implementation plan. "Good faith" in this context refers to a sincere intention to comply with Reliability Standard MOD-032-2 Requirement R2 Part 2.1, following a reasonable and serious assessment by the entity in determining how this Reliability

Standard should be applied to its particular facts and circumstances. For example, the CEA may not pursue compliance enforcement actions during this period for entities who submit estimated data and include the supporting data explanation and methods used as detailed in Requirement R2 Part 2.1 in a timely manner. The CEA may pursue actions against entities who do not submit data with supporting explanation and methods in a timely manner. Entities shall participate in any compliance monitoring activities undertaken by the CEA during this potential noncompliance abeyance period and submit documentation as requested.

Violation Severity Levels

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

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	reporting procedures, but did provide the data in less than or equal to 15 calendar days after the specified date.	data requirements and reporting procedures, but did provide the data in greater than 15, but less than or equal to 30 calendar days after the specified date.	data requirements and reporting procedures, but did provide the data in greater than 30, but less than or equal to 45 calendar days after the specified date.	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner or Transmission Service Provider failed to provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) within the schedule specified by the data requirements and reporting procedures, but did provide the data in greater than 45 calendar days after the specified date.
R3.	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R3 within 90 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner), but did provide the	The Balancing Authority, Distribution Provider, Generator Owner, Resource Planner, Transmission Owner, or Transmission Service Provider failed to provide a written response to its Transmission Planner(s) or Planning Coordinator(s) according to the specifications of Requirement R3 within 135 calendar days (or within a longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	response within 105 calendar days (or within 15 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	response within greater than 105 calendar days, but less than or equal to 120 calendar days (or within greater than 15 calendar days, but less than or equal to 30 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	response within greater than 120 calendar days, but less than or equal to 135 calendar days (or within greater than 30 calendar days, but less than or equal to 45 calendar days after the longer period agreed upon by the notifying Planning Coordinator or Transmission Planner).	
R4.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide less than or equal to 25% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 25%, but less than or equal to 50% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 50%, but less than or equal to 75% of the required data in the format specified by the ERO or its designee.	The Planning Coordinator made available the required data to the ERO or its designee, but failed to provide greater than 75% of the required data in the format specified by the ERO or its designee.

D. Regional Variances

None.

E. Associated Documents

- Project 2022-02 Implementation Plan
- Project 2022-02 Technical Rationale
- ERO Unacceptable Models List

MOD-032-2 – ATTACHMENT 1
Data Reporting Requirements

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

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics**	**short circuit**
1. Each bus [TO] a. Nominal voltage b. Area, zone and owner 2. Aggregate Demand[3] [DP] a. Real and reactive power* b. In-service status* 3. Generating and storage units[4] [GO, TO[5], RP (for future planned resources only)] a. Real power capabilities - gross maximum and minimum values b. Reactive power capabilities - maximum and minimum values at real power capabilities in 3a above c. Station service auxiliary load for normal plant configuration (provide data in the same manner as that required for aggregate Demand under item 2, above). d. Regulated bus* and voltage set point* (as typically provided by the TOP) e. Machine MVA base f. Generator step up transformer data (provide same data as that required for transformer under item 6, below) g. Generator type (hydro, wind, fossil, solar, nuclear, etc.) h. In-service status* 4. AC Transmission Line or Circuit [TO] a. Impedance parameters (positive sequence)	1. Generator [GO, RP (for future planned resources only)] 2. Excitation System [GO, RP (for future planned resources only)] 3. Governor [GO, RP (for future planned resources only)] 4. Power System Stabilizer [GO, RP (for future planned resources only)] 5. Aggregate Demand[3] [DP] 6. Wind plant model (for plants with type 1 and type 2 wind turbines) [GO] 7. Inverter-Based Resource [GO, TO[5]] a. Parameters, settings, or capabilities related to momentary cessation, tripping, Ride-through, voltage control, and frequency control 8. Static Var Systems and FACTS [GO, TO, DP] 9. DC System Models [TO] 10. Aggregate Distributed Energy Resource (DER) data[7] [DP, TO][6] a. parameters, settings, or capabilities related to momentary cessation, tripping, Ride-through, voltage control, and frequency control or information that can be used to infer those items for modeling purposes. b. Indication whether DERs are subject to tripping in conjunction with UFLS or UVLS.	1. Provide for all applicable elements in column "steady-state" [GO, RP, TO, DP] a. Positive sequence data b. Negative sequence data c. Zero sequence data 2. Mutual Line Impedance Data [TO] 3. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]

steady-state *(Items marked with an asterisk indicate data that vary with system operating state or conditions. Those items may have different data provided for different modeling scenarios)*	**dynamics**	**short circuit**
b. Susceptance (line charging) c. Ratings (normal and emergency)* d. In-service status* 5. DC Transmission Systems [TO] 6. Transformer (voltage and phase-shifting) [TO] a. Nominal voltages of windings b. Impedance(s) c. Tap ratios (voltage or phase angle)* d. Minimum and maximum tap position limits e. Number of tap positions (for both the ULTC and NLTC) f. Regulated bus (for voltage regulating transformers)* g. Ratings (normal and emergency)* h. In-service status* 7. Reactive compensation (shunt capacitors and reactors) [TO] a. Admittances (MVars) of each capacitor and reactor b. Regulated voltage band limits* (if mode of operation not fixed) c. Mode of operation (fixed, discrete, continuous, etc.) d. Regulated bus* (if mode of operation not fixed) e. In-service status* 8. Static Var Systems [TO] a. Reactive limits b. Voltage set point* c. Fixed/switched shunt, if applicable d. In-service status* 9. Aggregate Distributed Energy Resource (DER) data[7] [DP, TO][6] a. Location (bus from item 1) b. Real power capability c. DER type (solar, battery, diesel generator, etc.) 10. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]	11. Other information requested by the Planning Coordinator or Transmission Planner necessary for modeling purposes. [BA, GO, DP, TO, TSP]	

Attachment 1 Data Reporting Requirements Footnotes

1. Data specified in the sub-bullets of each column that are required for both steady-state and dynamics are not duplicated in the table.
2. For purposes of this attachment, the functional entity references are represented by abbreviations as follows: Balancing Authority (BA), Distribution Provider (DP), Generator Owner (GO), Planning Coordinator (PC), Resource Planner (RP), Transmission Owner (TO), Transmission Planner (TP), and Transmission Service Provider (TSP).
3. For purposes of this item, aggregate Demand is the gross Demand aggregated at each bus under item 1 under Steady State Column that is identified by a Transmission Owner as a load serving bus rather than the net Demand that incorporates offsets due to output from Distributed Energy Resources. (Note: This may be impacted by an aggregation threshold for DER specified under footnote 7.) A Distribution Provider is the typical responsible entity for providing this information, generally through coordination with the Transmission Owner.
4. Generating and storage units include IBRs and synchronous condensers.
5. The Transmission Owner is the typical entity responsible for collecting and providing data for an IBR that is not a DER and does not meet the criteria that would require the owner to register with NERC for mandatory Reliability Standards compliance purposes.
6. The Distribution Provider is the typical responsible entity for collecting and providing data for DERs connected to its system either directly or through an unregistered Distribution Provider (i.e., not included on the NERC Compliance Registry) with no other registered entity systems between the DER connection point and the Distribution Provider's system. The Transmission Owner is the typical responsible entity for collecting and providing data for DERs where there is no associated registered Distribution Provider between the DER connection point and the Transmission Owner's system.
7. Aggregation thresholds for DERs may be specified in the joint Planning Coordinator/Transmission Planner modeling data requirements and reporting procedures developed under Requirement R1.

MOD-032 Supporting Document

Process for Updating the Unacceptable Models List Maintained by the Electric Reliability Organization (ERO)

The Unacceptable Models List is maintained separately by NERC as the ERO. This Supporting Document describes the process by which changes may be made to the Unacceptable Models List. This process may only be revised through the NERC Standards Development Process.

The following steps shall be taken to add a model to or remove a model from the Unacceptable Models List:

1. Any person or entity may submit a request to the ERO to add or remove a model from the Unacceptable Models List. This request shall include, at a minimum:
    a. The model name;
    b. Alternative model name(s), if any;
    c. Organization(s) the submitting entity represents;
    d. Description of the model's stated intent;
    e. Request to add model as an "unacceptable" model or remove "unacceptable" model designation;
    f. Technical supporting documentation describing the ability or inability of the model to appropriately represent small and large disturbance behavior;
    g. Identification of any Confidential Information as defined in Section 1500 of the NERC Rules of Procedure; and
    h. An explanation, if any of the above technical support items are unavailable to the submitting entity.
2. ERO staff shall review and evaluate the information in the Unacceptable Models List change request, along with any group or subcommittee of the NERC Reliability and Security Technical Committee, or its successor (RSTC), charged with assisting in such reviews. If no such group or subcommittee has been identified, ERO staff may work with other industry subject matter experts as needed to review and evaluate the request.
3. ERO staff shall provide public notice that identifies the model being considered for addition to or removal from the list, includes a non-confidential summary of the rationale offered, and provides at least 30 days to submit comments.
4. The results of the ERO review and the recommended action shall be presented to the NERC RSTC in a duly noticed public meeting.
5. The NERC RSTC may recommend the NERC Vice President of Engineering and Standards approve the change request, reject the change request, or remand the application back to the ERO to work with the submitting entity. If the NERC RSTC recommends approving the change request, the NERC RSTC shall also recommend an effective date for the change.

6. The NERC Vice President of Engineering and Standards, considering the recommendation of the NERC RSTC, shall approve the change request, reject the change request, or remand the application back to ERO staff to work with the submitting entity. If approved, the NERC Vice President of Engineering and Standards shall also determine the effective date for the change.
7. The ERO shall provide public notice of a change to the Unacceptable Models List along with the effective date of the change. The revised Unacceptable Models List shall be posted to the NERC website and filed with the applicable governmental authorities for informational purposes.

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees.	Developed to consolidate and replace MOD-010-0, MOD -011-0, MOD-012-0, MOD-013-1, MOD-014-0, and MOD-015-0.1
1	May 1, 2014	FERC Order issued approving MOD-032-1.	See Implementation Plan posted on the Reliability Standards web page for details on enforcement dates for Requirements.
2	October 31, 2025	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2022-02.
2	TBD	FERC approved	

Reliability Standard IRO-010-6

A. Introduction

1. **Title:** Reliability Coordinator Data and information Specification and Collection
2. **Number:** IRO-010-6
3. **Purpose:** To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring each Reliability Coordinator has the data and information it needs to plan, monitor and assess the operation of its Reliability Coordinator Area.
4. **Applicability:**
   - **4.1.** Reliability Coordinator
   - **4.2.** Balancing Authority
   - **4.3.** Generator Owner
   - **4.4.** Generator Operator
   - **4.5.** Transmission Operator
   - **4.6.** Transmission Owner
   - **4.7.** Distribution Provider
5. **Effective Date:** See Implementation Plan for Project 2022-02.

B. Requirements

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

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

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

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

1.3.1 Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints.

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

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

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

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

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

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

1.5.3 Requirements for necessary model submissions to be consistent with the model submitted for planning purposes, subject to modifications for operations purposes, as applicable;

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

1.5.5 A mutually agreeable format; and

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

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

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

Violation Severity Levels

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	October 17, 2008	Adopted by Board of Trustees	New
1a	August 5, 2009	Added Appendix 1: Interpretation of R1.2 and R3 as approved by Board of Trustees	Addition
1a	March 17, 2011	FERC Order issued approving IRO-010-1a (approval effective 5/23/11)	
1a	November 19, 2013	Updated VRFs based on June 24, 2013 approval	
2	November 13, 2014	Adopted by NERC Board of Trustees	Revisions under Project 2014-03
2	November 19, 2015	FERC Order approving IRO-010-2. Docket No. RM15-16-000	
3	February 6, 2020	Adopted by NERC Board of Trustees	Revisions under Project 2017-07
3	October 30, 2020	FERC Order approving IRO-010-3. Docket No. RD20-4-000	
4	March 22, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	June 11, 2021	Adopted by NERC Board of Trustees	Revisions under Project 2019-06
4	August 24, 2021	FERC Order approving IRO-010-4. Docket No. RD21-5-000	
5	August 17, 2023	Adopted by NERC Board of Trustees	Revision under project 2021-06
5	November 2, 2023	FERC approved IRO-010-5. Docket No. RD23-6-000	
6	October 31, 2025	Adopted by NERC Board of Trustees	FERC Order 901 Modifications
6	TBD	FERC approved	

Reliability Standard TOP-003-8

A. Introduction

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

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

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

4. **Applicability:**

   4.1 Functional Entities:

   4.1.1 Transmission Operator

   4.1.2 Balancing Authority

   4.1.3 Generator Owner

   4.1.4 Generator Operator

   4.1.5 Transmission Owner

   4.1.6 Distribution Provider

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

B. Requirements and Measures

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

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

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

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

1.3.1. Operating limitations based on:

1.3.1.1. capability and availability;

1.3.1.2. fuel supply and inventory concerns;

1.3.1.3. fuel switching capabilities; and

1.3.1.4. environmental constraints

1.3.2. Generating unit(s) minimum:

1.3.2.1. design temperature; or

1.3.2.2. historical operating temperature; or

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

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

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

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

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

1.5.3. Requirements for necessary model submissions to be consistent with the model submitted for planning purposes, subject to modifications for operations purposes, as applicable;

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

1.5.5. A mutually agreeable format;

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

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

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

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

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

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

2.3.1. Operating limitations based on:

2.3.1.1. capability and availability;

2.3.1.2. fuel supply and inventory concerns;

2.3.1.3. fuel switching capabilities; and

2.3.1.4. environmental constraints.

2.3.2. Generating unit(s) minimum:

2.3.2.1. design temperature; or

2.3.2.2. historical operating temperature; or

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

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

2.5. Methods for the entity identified in Part 2.1 to provide data and information that includes, but is not limited to:

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

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

2.5.3. Requirements for necessary model submissions to be consistent with the model submitted for planning purposes, subject to modifications for operations purposes, as applicable;

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

2.5.5. A mutually agreeable format.

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

- Each Transmission Operator shall retain its dated, current, in force, documented specification for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R1 and Measurement M1 as well as any documents in force since the last compliance audit.
- Each Balancing Authority shall retain its dated, current, in force, documented specification(s) for the data and information necessary for it to perform its analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R2 and Measurement M2, as well as any documents in force since the last compliance audit.
- Each Transmission Operator shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Transmission Operator's Operational Planning Analyses, Real-time monitoring, and Real-time Assessments in accordance with Requirement R3 and Measurement M3.
- Each Balancing Authority shall retain evidence for three calendar years that it has distributed its specification(s) to entities that have data required by the Balancing Authority's analysis functions, Real-time monitoring, and Near-Term Energy Reliability Assessments in accordance with Requirement R4 and Measurement M4.
- Each Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R3 or R4 shall retain evidence for the most recent 90-calendar days that it has satisfied the obligations of the documented specifications in accordance with Requirement R5 and Measurement M5.

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

Violation Severity Levels

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

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

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

Version	Date	Action	Change Tracking
		No.RD25-5-000	
8	October 31, 2025	Adopted by the NERC Board of Trustees	Revisions to address FERC Order No. 901 directives
8	TBD	FERC approved	

Reliability Standard MOD-033-3

A. Introduction

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

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

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

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator

   4.1.2. Reliability Coordinator

   4.1.3. Transmission Operator

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

B. Requirements and Measures

R1. Each Planning Coordinator shall implement a documented Model Validation process for planning System models developed in accordance with Reliability Standard MOD-032,[1] representing its portion of the existing System, that includes the following attributes: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

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

1.2. Comparison of the dynamic local event simulation performance of the dynamic planning System model to actual System behavior, represented by Real-time data sources such as Disturbance data recording(s), at least once every 24 calendar months (using a dynamic local event that occurs within 24 calendar months of the last dynamic local event used in comparison) and completing each comparison within 24 calendar months of the dynamic local event. If no dynamic local event occurs within this 24 calendar months period, use the next dynamic local event that occurs.

1.3. Guidelines to determine unacceptable differences in performance under Parts 1.1 and 1.2 including those for generating facilities in the planning System model; and

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

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

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

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

[1] Such planning System models will thus include registered IBRs and aggregated DERs, as well as IBRs that are not DERs and that do not meet the criteria that would require the owner(s) to register with NERC for mandatory Reliability Standards compliance purposes, that are present in the existing System.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

The applicable entity shall keep data or evidence to show compliance with Requirements R1 and R2, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				but actually had the data, to a requesting Planning Coordinator.

D. Regional Variances

None.

E. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	February 6, 2014	Adopted by the NERC Board of Trustees	Developed as a new standard for system validation to address outstanding directives from FERC Order No. 693 and recommendations from several other sources.
1	May 1, 2014	FERC Order issued approving MOD-033-1.	
2	February 6, 2020	Adopted by the NERC Board of Trustees.	Revisions under Project 2017-07
2	October 30, 2020	FERC Order approving MOD- 033-2. Docket No. RD20-4-000	
3	October 31, 2025	Adopted by the NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2021-01
3	TBD	FERC approved	

Reliability Standard MOD-026-2

A. Introduction

1. **Title:** Verification and Validation of Dynamic Models and Data

2. **Number:** MOD-026-2

3. **Purpose:** To verify and validate that the dynamic models and associated parameters used to assess Bulk Electric System (BES) reliability represent the in-service equipment of Bulk Power System (BPS) facilities including generating facilities, transmission connected dynamic reactive resources, and high-voltage direct current (HVDC) systems.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Generator Owner

   4.1.2. Planning Coordinator

   4.1.3. Transmission Owner

   4.1.4. Transmission Planner

   4.2. Facilities:

   4.2.1. Individual synchronous generating unit meeting the criteria set by Inclusion I2 of the BES definition;

   4.2.2. Synchronous generating plant/Facility meeting the criteria set by Inclusion I2 of the BES definition;

   4.2.3. Dynamic reactive resources meeting the criteria set by Inclusion I5 of the BES definition with a gross (individual or aggregate) nameplate rating greater than 20 MVA including:

   4.2.3.1. Synchronous condensers; and

   4.2.3.2. Flexible alternating current transmission system (FACTS) devices.

   4.2.4. High-voltage direct current (HVDC) systems including:

   4.2.4.1. Line commutated converter (LCC); and

   4.2.4.2. Voltage source converter (VSC).

   4.2.5. Bulk Electric System (BES) Inverter-Based Resources; and

   4.2.6. Non-BES Inverter-Based Resources that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV.

   4.2.7. Non-synchronous generating plant/Facility meeting the criteria set by Inclusion I4 of the BES definition.

5. **Effective Date:** See Implementation Plan for Project 2020-06 Verifications of Models and Data for Generators.

B. Requirements and Measures

R1. Each Transmission Planner and its Planning Coordinator shall jointly develop dynamic model requirements for the purpose of evaluating submitted dynamic models and accompanying documentation of Model Verification and Model Validation. The dynamic model requirements shall be made available to Generator Owner(s) and Transmission Owner(s) by the Transmission Planner and shall include at a minimum the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. Positive sequence dynamic model requirements, including requirements for the models and functions listed in Attachment 1;

1.1.1. Specification of which limiting and protective functions listed within Attachment 1, Table 1.1 are required to be represented in the model.

1.2. For the facilities listed in Applicability Sections 4.2.5 and 4.2.6 (Inverter-Based Resources), 4.2.3.2 (FACTS devices), 4.2.4.1 (LCC HVDC), and 4.2.4.2 (VSC HVDC):

1.2.1. Identification of which legacy[1] facilities require electromagnetic transient (EMT) model(s) under Requirement R3 accompanied by a statement of need; and

1.2.2. Specification of acceptable EMT models, format, and level of detail.

1.3. Any additional requirements not listed under Requirement R1, Parts 1.1 and 1.2 used by the Transmission Planner to determine the acceptability of submitted dynamic models and accompanying documentation under Requirement R5. If no such additional requirements exist, the Transmission Planner shall document that none are applicable.

M1. Each Transmission Planner and Planning Coordinator must provide dated evidence such as document(s), webpage(s), or web portal(s) outlining the jointly developed dynamic model requirements. Each Transmission Planner shall have evidence demonstrating that the dynamic model requirements were made available to Generator Owner(s) and Transmission Owner(s) in accordance with Requirement R1.

R2. Each Generator Owner or Transmission Owner shall provide to its Transmission Planner positive sequence dynamic model(s) with associated parameters, any information pertaining to changes to the model(s) or its parameters, and accompanying documentation in accordance with the periodicity requirements of Attachment 2. Each Generator Owner or Transmission Owner shall provide the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. Positive sequence dynamic model(s) representing the in-service equipment of the facility including, at a minimum, each of the applicable models and functions listed in Attachment 1 in accordance with the requirements developed in Requirement R1;

2.2. Documentation of Model Verification demonstrating that the configurable, site-specific parameters of the model(s) are representative of the design and settings of the in-service equipment of the facility;

[1] A legacy facility for the purpose of this standard is any facility with a commercial operation date prior to the effective date of MOD-026-2.

2.2.1. For any parameters that cannot be verified, the Generator Owner or Transmission Owner shall provide a written statement to the Transmission Planner identifying the unverifiable parameters and reasons they cannot be verified.

2.3. Documentation of Model Validation comparing the behavior of the model(s) to the measured behavior during a staged test or system disturbance for:

2.3.1. A dynamic reactive power or voltage excursion event to perform Model Validation of generator, excitation control, reactive power control, and voltage control models, as applicable; and

2.3.2. A dynamic active power or frequency excursion event to perform Model Validation of governor control, active power control, and frequency control models, as applicable. For a frequency excursion event to be sufficient for Model Validation, the applicable facility must be operating in a frequency responsive mode and the frequency deviation (nadir point) from the scheduled frequency must be greater than or equal to:

2.3.2.1. 0.04 hertz in the Eastern Interconnection;

2.3.2.2. 0.08 hertz in the ERCOT and Western Interconnections; and

2.3.2.3. 0.30 hertz in the Quebec Interconnection.

M2. Each Generator Owner or Transmission Owner must provide dated evidence (e.g., email message, postal receipt, upload via web portal, etc.) for each applicable facility that it provided positive sequence dynamic model(s) and accompanying documentation to its Transmission Planner in accordance with Requirement R2.

R3. For facilities listed in Applicability Sections 4.2.3.2 (FACTS devices), 4.2.4 (HVDC), 4.2.5 (BES IBRs), and 4.2.6 (Non-BES IBRs), excluding legacy facilities where the original equipment manufacturer[2] no longer supports EMT model(s) for the facility as well as legacy facilities not identified by the Transmission Planner under Requirement R1, Part 1.2.1, each Generator Owner or Transmission Owner shall provide to its Transmission Planner EMT model(s) with associated parameters, any information pertaining to changes to the model(s) or its parameters, and accompanying documentation, in accordance with the periodicity requirements of Attachment 2. Each Generator Owner or Transmission Owner shall provide the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. A facility EMT model with associated parameters representing the applicable HVDC, FACTS device, IBR unit(s),[3] collector system, auxiliary control device(s),[4] power plant controller, generator step-up transformer(s), and main power transformer(s) that includes:

[2] If the original equipment manufacturer that commissioned the facility was acquired, merged, or operating under a different name, the new company would be considered the original equipment manufacturer.

[3] For purposes of this standard, the phrase "IBR unit" refers to an individual device, or a grouping of multiple devices, that uses a power electronic interface(s), such as an inverter or converter, that is capable of exporting Real Power from a primary energy source or energy storage system, and that connects at a single point on the collector system.

[4] Only to include those auxiliary control devices that act on voltage and/or frequency.

3.1.1. Enabled protective functions[5] that directly trip the IBR unit(s) or facility; and

3.1.2. Limiting functions[6] that limit active/reactive output of the IBR unit(s) or facility.

3.2. Documentation of Model Verification demonstrating that the configurable, site-specific parameters of the model(s) are representative of the design and settings of the in-service equipment of the facility;

3.2.1. For any parameters that cannot be verified, the Generator Owner or Transmission Owner shall provide a written statement to the Transmission Planner identifying the unverifiable parameters and reasons they cannot be verified.

3.3. Documentation of Model Validation comparing the behavior of the facility EMT model to the measured behavior during a staged test or system disturbance for:

3.3.1. A dynamic reactive power or voltage excursion event to perform Model Validation of reactive power control and voltage control models, as applicable; and

3.3.2. A dynamic active power or frequency excursion event to perform Model Validation of active power control and frequency control models, as applicable. For a frequency excursion event to be sufficient for Model Validation, the applicable facility must be operating in a frequency responsive mode and the frequency deviation (nadir point) from the scheduled frequency must be greater than or equal to:

3.3.2.1. 0.04 hertz in the Eastern Interconnection;

3.3.2.2. 0.08 hertz in the ERCOT and Western Interconnections; and

3.3.2.3. 0.30 hertz in the Quebec Interconnection.

3.4. For IBR facilities, test[7] result(s) demonstrating a comparison of the IBR unit response and the IBR unit EMT model response for large signal disturbances. If test results are not obtainable, the Generator Owner shall document the reason; and

3.5. Documentation comparing the response of the facility positive sequence dynamic model provided in Requirement R2 to the response of the facility EMT model for large signal disturbances as defined by the Transmission Planner.

M3. Each Generator Owner or Transmission Owner must provide dated evidence (e.g., email message, postal receipt, upload via web portal, etc.) for each applicable facility that it provided EMT model(s) and accompanying documentation to its Transmission Planner in accordance with Requirement R3.

---

[5] Required protective functions are those that act directly on, or act on quantities derived from, voltage, frequency, and/or current. Examples of protections include DC reverse current, DC bus over-voltage and under-voltage, DC voltage unbalance, DC overcurrent, AC over-voltage and under-voltage protection (instantaneous and RMS), AC overcurrent, over-frequency and under-frequency protection, feeder (equivalent) AC over-voltage and under-voltage, feeder (equivalent) over-frequency and under-frequency, PLL (or equivalent) loss of synchronism, and phase jump tripping.

[6] Required limiting functions are those that act directly on, or act on quantities derived from, voltage, frequency, and/or current.

[7] A hardware specific test may include a factory type test, hardware in the loop test, or other manufacturer test to ensure the EMT model's large signal response emulates the supplied equipment to the extent possible.

R4. Each Generator Owner or Transmission Owner shall, within 180 calendar days after making a hardware, software, firmware, control mode, or setting change(s)[8] to an applicable unit or facility that alters the dynamic response characteristic(s), provide its Transmission Planner with updated model(s) and accompanying documentation as described in Requirement R2, Parts 2.1 through 2.3 and, if applicable, Requirement R3, Parts 3.1 through 3.5. If mutually agreed upon with the Transmission Planner, model(s) and accompanying documentation may be provided according to a revised timeline. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Each Generator Owner or Transmission Owner must provide dated evidence (e.g., email message, postal receipt, upload via web portal, etc.) that it provided its Transmission Planner with updated model(s) and accompanying documentation in accordance with Requirement R4 for each change altering dynamic response characteristic(s) of an applicable unit or facility.

R5. Each Transmission Planner shall, within 120 calendar days after receiving model(s) and accompanying documentation provided by a Generator Owner or Transmission Owner or within a mutually agreed upon timeline with the applicable Generator Owner or Transmission Owner, evaluate the model(s) and accompanying documentation to determine if it meets the dynamic model requirements developed under Requirement R1 and provide: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- A written notification to the Generator Owner or Transmission Owner that the model(s) and accompanying documentation are acceptable, and a written notification, or the accepted model(s) and accompanying documentation, to its Planning Coordinator; or
- A written notification to the Generator Owner or Transmission Owner that the model(s) and accompanying documentation are not acceptable, along with an explanation and any supporting evidence demonstrating the issue(s).

M5. Each Transmission Planner must provide dated evidence that it reviewed provided model(s) and accompanying documentation in accordance with the dynamic model requirements developed in Requirement R1 and provided a written response notification in accordance with Requirement R5. Dated evidence may include date received, review date of provided model(s) and accompanying documentation, and dated response (e.g., email message, postal receipt, etc.).

R6. Each Generator Owner or Transmission Owner shall, within 120 calendar days after receiving a notification of unacceptability under Requirement R5 or within 180 calendar days after receiving a request from its Transmission Planner to perform a model review due to identified model or accompanying documentation deficiencies, provide a response to its Transmission Planner. If mutually agreed upon with the Transmission Planner, the response to a request to perform a model review may be provided according to a revised timeline. The provided response shall include one of the following: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- Updated model(s) and accompanying documentation as described in Requirement R2, Parts 2.1 through 2.3 and, if applicable, Requirement R3, Parts 3.1 through 3.5; or

[8] Automatic changes in settings that occur due to changes in operating mode are excluded from Requirement R4.

- A technical justification and supporting evidence for maintaining the current model(s) and accompanying documentation.

M6. Each Generator Owner or Transmission Owner must provide dated evidence (e.g., email message, postal receipt, etc.) that it provided a response to its Transmission Planner in accordance with Requirement R6.

R7. Each Transmission Planner shall provide the current (in-use) model(s) and accompanying documentation for an existing facility within 90 calendar days of receiving a written request for such data from the Generator Owner or Transmission Owner that owns the facility. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M7. Each Transmission Planner must provide dated evidence (e.g., email message, postal receipt, etc.) that it provided the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner in accordance with Requirement R7.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

- Requirements R1 through R7, and Measures M1 through M7, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer. The Compliance Enforcement Authority shall keep the last audit records, and all requested and submitted subsequent audit records.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Transmission Planner and Planning Coordinator jointly developed dynamic model requirements, but they failed to include one of the items in Requirement R1, Parts 1.1 through 1.3.	The Transmission Planner and Planning Coordinator jointly developed dynamic model requirements, but they failed to include two of the items in Requirement R1, Parts 1.1 through 1.3.	The Transmission Planner and Planning Coordinator jointly developed dynamic model requirements, but they failed to include three of the items in Requirement R1, Parts 1.1 through 1.3. OR The Transmission Planner and Planning Coordinator failed to jointly develop dynamic model requirements. OR The Transmission Planner failed to make dynamic model requirements available to Generator Owners and Transmission Owners.
R2.	The applicable entity provided positive sequence dynamic model(s), with associated parameters, and accompanying documentation to its Transmission Planner in accordance with the periodicity requirements of Attachment 2 with the exception of Row 2, but within	The applicable entity provided positive sequence dynamic model(s), with associated parameters, and accompanying documentation to its Transmission Planner between 91 and 180 calendar days after the date in accordance with the periodicity requirements of	The applicable entity provided positive sequence dynamic model(s), with associated parameters, and accompanying documentation to its Transmission Planner between 181 and 270 calendar days after the date in accordance with the periodicity requirements of	The applicable entity provided positive sequence dynamic model(s), with associated parameters, and accompanying documentation to its Transmission Planner more than 270 calendar days after the date in accordance with the periodicity requirements of Attachment 2 with the exception of Row 2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	90 calendar days after the date required. OR The applicable entity provided dynamic model(s) that failed to include one of the applicable items in Attachment 1, Table 1.1 or Table 1.2.	Attachment 2 with the exception of Row 2. OR The applicable entity provided dynamic model(s) that failed to include two of the applicable items in Attachment 1, Table 1.1 or Table 1.2.	Attachment 2 with the exception of Row 2. OR The applicable entity provided dynamic model(s) that failed to include three of the applicable items in Attachment 1, Table 1.1 or Table 1.2.	OR The applicable entity failed to provide dynamic model(s) or accompanying information.
R3.	The applicable entity provided EMT model(s) for its applicable facility with associated parameters and accompanying documentation to its Transmission Planner, in accordance with the requirements developed by its Transmission Planner and Planning Coordinator, after the date required but within 90 calendar days after the date required. OR The applicable entity provided EMT model(s) and accompanying documentation by the required date, but failed to include one of the items in Requirement R3, Parts 3.1 through 3.5.	The applicable entity provided EMT model(s) for its applicable facility with associated parameters and accompanying documentation to its Transmission Planner, in accordance with the requirements developed by its Transmission Planner and Planning Coordinator, between 91 and 180 calendar days after the date required. OR The applicable entity provided EMT model(s) and accompanying documentation by the required date, but failed to include two of the items in Requirement R3, Parts 3.1 through 3.5.	The applicable entity provided EMT model(s) for its applicable facility with associated parameters and accompanying documentation to its Transmission Planner, in accordance with the requirements developed by its Transmission Planner and Planning Coordinator, between 181 and 270 calendar days after the date required. OR The applicable entity provided EMT model(s) and accompanying documentation by the required date, but failed to include three of the items in Requirement R3, Parts 3.1 through 3.5.	The applicable entity provided EMT model(s) for its applicable facility with associated parameters and accompanying documentation to its Transmission Planner, in accordance with the requirements developed by its Transmission Planner and Planning Coordinator, more than 270 calendar days after the date required. OR The applicable entity provided EMT model(s) by the required date, but failed to include four of the items in Requirement R3, Parts 3.1 through 3.5. OR The applicable entity failed to provide EMT model(s) and accompanying documentation.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	The applicable entity provided updated model(s) and accompanying documentation to its Transmission Planner between 181 and 210 calendar days (or within 30 calendar days after the timeline mutually agreed to by the Transmission Planner) after making a change that alters the dynamic response characteristic(s).	The applicable entity provided updated model(s) and accompanying documentation between 211 and 240 calendar days (or between 31 and 60 calendar days after the timeline mutually agreed to by the Transmission Planner) after making a change that alters the dynamic response characteristic(s).	The applicable entity provided updated model(s) and accompanying documentation between 241 and 270 calendar days (or between 61 and 90 calendar days after the timeline mutually agreed to by the Transmission Planner) after making a change that alters the dynamic response characteristic(s).	The applicable entity provided updated model(s) and accompanying documentation more than 270 calendar days (or more than 90 calendar days after the timeline mutually agreed to by the Transmission Planner) after making a change that alters the dynamic response characteristic(s). OR The applicable entity failed to identify, provide updated model(s) and accompanying documentation after making a change that alters the dynamic response characteristic(s).
R5.	The Transmission Planner reviewed the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, but provided a written response to the submitter between 121 to 150 calendar days (or within 30 calendar days after the timeline mutually agreed to by the Generator Owner or	The Transmission Planner reviewed the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, but provided a written response to the submitter between 151 to 180 calendar days (or within 31 and 60 calendar days after the timeline mutually agreed to by the Generator Owner or	The Transmission Planner reviewed the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, but provided a written response to the submitter between 181 to 210 calendar days (or within 61 and 90 calendar days after the timeline mutually agreed to by the Generator Owner or	The Transmission Planner reviewed the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, but provided a written response to the submitter more than 210 calendar days (or more than 90 calendar days after the timeline mutually agreed to by the Generator Owner or

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Transmission Owner) after receiving the submission.	Transmission Owner) after receiving the submission.	Transmission Owner) after receiving the submission.	Transmission Owner) after receiving the submission. OR The Transmission Planner reviewed the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, and provided a response indicating that the model was unacceptable, but did not include an explanation and supporting evidence. OR The Transmission Planner failed to review the submitted model(s) and accompanying documentation for adherence to the dynamic model requirements developed in Requirement R1, and failed to provide a response to the submitter.
R6.	The applicable entity provided a response to the Transmission Planner after receiving a notification of unacceptability under Requirement R5, but did so between 121 to 150	The applicable entity provided a response to the Transmission Planner after receiving a notification of unacceptability under Requirement R5, but did so between 151 to 180	The applicable entity provided a response to the Transmission Planner after receiving a notification of unacceptability under Requirement R5, but did so between 181 to 210	The applicable entity failed to provide a response to the Transmission Planner after receiving a notification of unacceptability under Requirement R5 or a request to perform a model review.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days after receiving a notification of unacceptability. OR The applicable entity provided a response to the Transmission Planner after receiving a request to perform a model review, but did so between 181 to 210 calendar days (or within 30 calendar days after the timeline mutually agreed to by the Transmission Planner) after receiving a request to perform a model review.	calendar days after receiving a notification of unacceptability. OR The applicable entity provided a response to the Transmission Planner after receiving a request to perform a model review, but did so between 211 to 240 calendar days (or between 31 and 60 calendar days after the timeline mutually agreed to by the Transmission Planner) after receiving a request to perform a model review.	calendar days after receiving a notification of unacceptability. OR The applicable entity provided a response to the Transmission Planner after receiving a request to perform a model review, but did so between 241 to 270 calendar days (or between 61 and 90 calendar days after the timeline mutually agreed to by the Transmission Planner) after receiving a request to perform a model review.	OR The applicable entity provided a response to the Transmission Planner after receiving a notification of unacceptability under Requirement R5, but did so more than 210 calendar days after receiving a notification of unacceptability. OR The applicable entity provided a response to the Transmission Planner after receiving a request to perform a model review, but did so more than 270 calendar days (or more than 120 calendar days after the timeline mutually agreed to by the Transmission Planner) after receiving a request to perform a model review. OR The applicable entity provided a response to the Transmission Planner after receiving a notification of unacceptability or a request to perform a model review, but its response failed to contain one of the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				two options for responses described in Requirement R6.
R7	The Transmission Planner provided the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner, but did so between 91 and 120 calendar days after receiving a request.	The Transmission Planner provided the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner, but did so between 121 and 150 calendar days after receiving a request.	The Transmission Planner provided the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner, but did so between 151 and 180 calendar days after receiving a request.	The Transmission Planner provided the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner, but did so more than 180 calendar days after receiving a request. OR The Transmission Planner failed to provide the current (in-use) model(s) and accompanying documentation to the Generator Owner or Transmission Owner after receiving a request.

D. Regional Variances

None.

E. Associated Documents

- Project 2020-06 Verifications of Models and Data for Generators Implementation Plan
- Project 2020-06 MOD-026-2 Technical Rationale
- Project 2020-06 VRF VSL Justifications Document
- Project 2020-06 Consideration of Directives

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees.	New
1	March 20, 2014	FERC Order issued approving MOD-026-1. (Order becomes effective for R1, R3, R4, R5, and R6 on 7/1/14. R2 becomes effective on 7/1/18.)	
1	May 7, 2014	NERC Board of Trustees adopted revisions to VSLs in Requirement R6.	Revisions
1	November 26, 2014	FERC issued a letter order approved revision to VSLs in Requirement R6.	
2	October 31, 2025	Adopted by NERC Board of Trustees.	FERC Order No. 901 Revisions by Project 2020-06.
2	TBD	FERC approved	

Attachment 1

Table 1.1 Applicability: Facility Sections 4.2.1 or 4.2.2 Synchronous Condenser Identified in Facility Section 4.2.3.1			
Generator Model	**Excitation Control**	**Governor Control**	**Additional Limiting and Protective Functions**
1. Manufacturer, model number (if available), and type of generator/synchronous condenser; 2. Models representing the generator/synchronous condenser.	1. Manufacturer, model number (if available), and type of excitation system hardware and control; 2. Model(s) representing the excitation system including voltage regulator, impedance compensation (such as droop, line drop, differential compensation), power system stabilizer, and outer-loop controls which impact dynamic volt/volt-ampere reactive (VAR) performance.	1. Manufacturer, model number (if available), and type of prime mover, governor, and control; 2. Model(s) representing the prime mover, governor control system, and any other controls which impact the dynamic active real power or frequency performance due to a system disturbance (e.g., load controller), but excluding Automatic Generation Control.	If required by its Transmission Planner under Requirement R1, Part 1.1.1, Generator Owner(s) or Transmission Owner(s) shall submit: 1. Model(s) representing enabled excitation limiters; 2. Model(s) representing enabled AC over-voltage, AC under-voltage, enabled over-frequency, under-frequency, over-speed, under-speed, Volts per Hertz protective functions, out of step protection that trip the excitation system, the prime mover, or generator/synchronous condenser either directly or via lockout or auxiliary tripping relays.

Table 1.2 Applicability: Facility Sections 4.2.5, 4.2.6 and 4.2.7 FACTS Devices Identified in Facility Section 4.2.3.2 HVDC Systems Identified in Facility Section 4.2.4			
The facility	**Volt/VAR Control**	**Frequency/ Power Control[9]**	**Additional Limiting and Protective Functions**
1. Manufacturer 2. Model Number (if available) 3. Software/Firmware versions for applicable facility's a. IBR unit(s) b. FACTS device(s) c. VSC HVDC d. LCC HVDC e. Power plant controller(s)	1. Model(s) representing associated reactive power/voltage control as applicable for the specific facility or equipment. a. In the case of IBR, the model shall include: i. IBR unit(s) electronic control ii. The facility's power plant control iii. Supplemental reactive power devices and their control b. Other equipment which impacts facility voltage and reactive power dynamic response.[10]	1. Model(s) representing the associated active power/frequency control including the specific facility or equipment. a. In the case of the IBR, the model shall include: i. IBR unit(s) electronic control ii. The facility's power plant control b. Other equipment which impacts facility active power or grid frequency dynamic response.[11]	1. Model(s) representing enabled limiting functions, which limit active or reactive output of the IBR unit or facility. Limiting functions include active or reactive power limiting, active or reactive current limiting, or other limiting functions as may be involved in active or reactive power prioritization, ramping, disturbance ride-through and post-disturbance recovery behaviors. 2. Model(s) representing enabled protection functions that directly trip IBR unit(s) or facility, to include AC over-voltage and under-voltage protection, and over-frequency and under-frequency protection.

[9] Not applicable for FACTS Devices identified in Facility Section 4.2.3.2
[10] This includes models such as induction generator dynamics and associated reactive compensation devices (e.g., capacitor banks, SVCs) in Type 1 and Type 2 wind turbine generators.
[11] This includes models such as induction generator dynamics, rotor resistance controls, and blade pitch controls in Type 1 and Type 2 wind turbine generators.

Attachment 2

Periodicity		
Row Number	**Triggering Condition**	**Required Action**
1	Establishing the initial verification date for an applicable facility. (Applies to Requirement R2 and Requirement R3)	For Requirement R2, transmit the model(s) and accompanying documentation meeting Requirement R2, Parts 2.1 through 2.3 to its Transmission Planner in accordance with the date(s) of the Implementation Plan. For Requirement R3, transmit the model(s) and accompanying documentation meeting Requirement R3, Parts 3.1 through 3.5 to its Transmission Planner in accordance with the date of the Implementation Plan or within 365 calendar days after the Transmission Planner identifies the facility as an applicable facility in accordance with Requirement R1, Part 1.2.1, whichever is later.
2	Initial verification for a newly commissioned facility. (Applies to Requirement R2 and Requirement R3)	Transmit the model(s) and accompanying documentation meeting Requirement R2, Parts 2.1 through 2.3 and, if applicable, Requirement R3, Parts 3.1 through 3.5 to its Transmission Planner within 365 calendar days after the commercial operation date.
3	Subsequent Model Validation and Model Verification for an applicable facility. (Applies to Requirement R2 and Requirement R3)	Transmit the model(s) and accompanying documentation meeting Requirement R2, Parts 2.1 through 2.3 and, if applicable, Requirement R3, Parts 3.1 through 3.5 to its Transmission Planner within 10 calendar years of the most recent transmittal.
4	Applicable facility with installed and operating recording equipment does not experience a frequency excursion as applicable per Requirement R2, Part 2.3.2 or Requirement R3, Part 3.3.2 by the date otherwise required to meet the dates per Attachment 2, Rows 1, 2, or 3.	Requirement R2, Part 2.3.2 and Requirement R3, Part 3.3.2 are met with a written statement transmitted to its Transmission Planner. Transmit the model(s) and accompanying documentation meeting Requirement R2, Parts 2.1 through 2.3 or Requirement R3, Parts 3.1 through 3.5 to its Transmission Planner on or before 365 calendar days after a frequency

Periodicity		
Row Number	**Triggering Condition**	**Required Action**
	(Applies to Requirement R2 and Requirement R3) This row applies only if a frequency excursion from a system disturbance that meets Requirement R2, Part 2.3.2 or Requirement R3, Part 3.3.2 is selected for the validation method and the ability to record the applicable unit's real power response to a frequency excursion is installed and expected to be available.	excursion per Requirement R2, Part 2.3.2 or Requirement R3, Part 3.3.2 occurs, and the recording equipment captures the applicable facility's active power response as expected.
5	For an existing applicable facility with a change to in-service equipment as described under Requirement R4. (Applies to Requirement R4)	In order for the transmittal to reset the 10-year anniversary transmittal date for Requirement R2 and Requirement R3 as described in Row 3, all model(s) and model parameters must be verified according to the applicable requirement(s) and included in the transmittal.
6	Existing, new, or upgraded synchronous generating unit or synchronous condenser that is equivalent to other unit(s) at the same physical location. AND Each unit has the same MVA nameplate rating; AND The nameplate rating is ≤ 350 MVA; AND Each unit has the same components, ratings, and settings; AND The model for one of these equivalent units has been verified. (Applies to Requirement R2)	Provide a written explanation and include with the model(s) and accompanying documentation provided to its Transmission Planner for the equivalent unit. Model Verification and Model Validation shall be performed for a different equivalent unit during each 10-year period.

Periodicity		
Row Number	**Triggering Condition**	**Required Action**
7	Applicable facility is not responsive to voltage excursion events during normal operation; OR New or existing applicable facility does not have an installed closed loop voltage or reactive power control function or has a disabled closed loop voltage or reactive power control system function. (Applies to Requirement R2, Part 2.3.1 or Requirement R3, Part 3.3.1)	Requirement R2, Part 2.3.1 and Attachment 1, Table 1.1, Excitation Control column or Table 1.2, Volt/VAR Control column and Requirement R3, Part 3.3.1 are met with a written statement to that effect transmitted to its Transmission Planner.
8	Applicable facility is not designed to be responsive to frequency excursion events during normal operation. (The applicable facility does not operate in a frequency control mode, except during normal start up and shut down, that would result in a prime mover/governor and load control or active power/frequency control mode response.) OR New or existing applicable facility does not have an installed frequency control system or has a disabled frequency control system. (Applies to Requirement R2, Part 2.3.2 or Requirement R3, Part 3.3.2) If the applicable facility is operating in a frequency control mode that is responsive to a frequency excursion event in only one direction (over- or under-frequency), then Requirement R2, Part 2.3.2 and Requirement R3, Part 3.3.2 are still applicable.	Requirement R2, Part 2.3.2 and Attachment 1, Table 1.1, Governor Control column or Table 1.2, Frequency/Power Control column and Requirement R3, Part 3.3.2 are met with a written statement to that effect transmitted to its Transmission Planner.
9	Existing applicable unit or facility, excluding synchronous condensers, FACTS devices, and HVDC facilities, has a	Requirements R2 or Requirement R3 are met with a written statement to that effect transmitted to its Transmission Planner

Periodicity		
Row Number	**Triggering Condition**	**Required Action**
	current average net capacity factor over the most recent three calendar years, beginning on January 1 and ending on December 31, of 5% or less. (Requirement R2 or Requirement R3 periodicity exemption of Row 3; does not exempt obligation under Requirement R4 or Requirement R6.)	annually. If the current average net capacity factor over the most recent three calendar years exceeds 5%, then transmit the model(s) and accompanying documentation meeting Requirement R2, Parts 2.1 through 2.3 and, if applicable, Requirement R3, Parts 3.1 through 3.5 within 365 calendar days. For the definition of net capacity[12] factor refer to Appendix F of the GADS Data Reporting Instructions.[13]

[12] Net Capacity Factor: **NCF** = [**Σ** (**Net Actual Generation**) / **Σ** (**N**et **M**aximum **C**apacity **x P**eriod **H**ours)] **x 100**%
Where, Period Hours = 8760 x 3 = 26280. In the case of batteries, the absolute value of discharging and charging shall be summed into Net Actual Generation.
[13] Refer to Appendix F of the GADS Conventional Data Reporting Instructions.
https://www.nerc.com/pa/RAPA/gads/DataReportingInstructions/Appendix_F_Equations_2025_DRI.pdf

Reliability Standard CIP-002-8

A. Introduction

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

2. **Number:** CIP-002-8

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-002-8:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-002

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 BCS according to Attachment 1, Section 1, if any, at each asset;

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	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 BCS, five percent or fewer of identified BCS 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 BCS, five or fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR	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 high and medium impact BCS, more than five percent, but less than or equal to 10 percent of identified BCS 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 BCS, more than	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 high or medium impact BCS, more than 10 percent, but less than or equal to 15 percent of identified BCS 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 BCS, more	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 BCS, more than 15 percent of identified BCS 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 BCS, more than 15 identified BCS have not been categorized or have been incorrectly categorized at

R #	Violation Severity Levels (CIP-002-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	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. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent, but less than or equal to 10 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five, but less than or equal to 10 high or medium BCS have not been identified.	than 10, but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent, but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 10, but less than or equal to 15 high or medium BCS have not been identified.	a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS 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 BCS have not been identified.
R2	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months, but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months, but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months, but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate

R #	Violation Severity Levels (CIP-002-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months, but less than or equal to 16 calendar months of the previous approval. (Part 2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months, but less than or equal to 17 calendar months of the previous approval. (Part 2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months, but less than or equal to 18 calendar months of the previous approval. (Part 2.2)	according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2021-03
- CIP-002-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12
7	5/9/2024	Adopted by the NERC Board of Trustees	Virtualization Modifications under Project 2016-02
8	12/10/2024	Adopted by the NERC Board of Trustees	Transmission Owners Control Centers Updates under Project 2021-03

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

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

1. **High impact rating**
   Each BCS used by and located at any of the following:

   1.1. For Reliability Coordinators, each Control Center or backup Control Center used to perform the reliability tasks of the Reliability Coordinator.

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

   1.3. For Transmission Operators and Transmission Owners, each Control Center or backup Control Center 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 For Generator Operators, each Control Center or backup Control Center used to perform the reliability tasks of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

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

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

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

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

   2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted

value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

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

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

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

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

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more 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 UVLS or UFLS under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. For Generator Operators, each Control Center or backup Control Center used to perform the reliability tasks 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. For Transmission Operators and Transmission Owners, each Control Center or backup Control Center 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 BES Transmission Line,” shown in the table below, for lines that are monitored and controlled by the Control Center or backup Control Center. Include each BES Transmission Line that is connected between two or more Transmission stations or substations.

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 (N/A)

Exclusion:
Provided that the "aggregate weighted value" calculated according to the table above is less than 12000, a Transmission Operator or a Transmission Owner may exclude the BES Transmission Lines that are contained in a single group of contiguous Elements from their "aggregate weighted value" calculation, where a group of contiguous Elements is defined as:

- a group of contiguous Elements emanating from multiple points of connection at 69 kV or higher;
- that are operated at less than 300 kV; and
- where the gross export does not exceed 75 MWh during non-Energy Emergency Alert conditions. The gross export is based on the hourly integrated values of the preceding 12 calendar months.

2.13. For Balancing Authorities, each Control Center or backup Control Center used to perform the reliability tasks of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

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

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

Reliability Standard CIP-003-11

A. Introduction

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

2. **Number:** CIP-003-11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority 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 Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient

Version	Date	Action	Change Tracking
			devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02
11	12/10/2024	Adopted by the NERC Board of Trustees	Modifications made by Project 2023-04

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including, but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Reliability Standard CIP-002-7

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

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

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

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

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

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

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards 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 BCS according to Attachment 1, Section 1, if any, at each asset;

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	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 BCS, five percent or fewer of identified BCS 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 BCS, five or	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 high and medium impact BCS, more than five percent but less than or equal to 10 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	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 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	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 BCS, more than 15 percent of identified BCS 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 BCS, more

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, 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. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high or medium impact BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	than 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS 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 BCS have not been identified.
R2	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-002-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	5/9/2024	Adopted by the NERC Board of Trustees.	Virtualization Modifications

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

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

1. **High impact rating**
   Each BCS used by and located at any of the following:

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

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

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

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

2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

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

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

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

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

   2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher

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

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

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

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

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

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

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

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

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

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

3. Low impact rating

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

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

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

Reliability Standard CIP-003-10

A. Introduction

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

2. **Number:** CIP-003-10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
10	5/9/2024	Adopted by the NERC Board of Trustees.	Virtualization Modifications under Project 2016-02

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Reliability Standard CIP-004-8

A. Introduction

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

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.
2.2	High impact BCS and their associated:	Require completion of the training	Examples of evidence may include, but are

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part	If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High impact BCS and their associated	For termination actions, revoke the	Examples of evidence may include, but are

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	EACMS SCI supporting an Applicable System in this Part	individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language

Version	Date	Action	Change Tracking
			and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	5/9/2024	Adopted by the NERC Board of Trustees	Virtualization Modifications by Project 2016-02

Reliability Standard CIP-005-8

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High impact BCS and their associated PCA	Have one or more method(s) to	Examples of evidence may include,

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	disable active vendor remote access (including IRA and system-to-system remote access).	but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for permitting communications. (Part 1.2)	The Responsible Entity did not document one or more processes for CIP-005-8 Table R1 – Electronic Security Perimeter. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications and deny all other communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces for Applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including IRA and system-to-system remote access) (Part 2.5).	(including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated	The Responsible Entity did not implement any processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	08/10/17	Adopted by the NERC Board of Trustees.	Modified to address certain directives in FERC Order No. 829.
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	11/05/2020	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 850.
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
8	5/9/2024	Approved by the NERC Board of Trustees.	Virtualization Modifications by Project 2016-02

Reliability Standard CIP-006-7.1

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

   4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

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

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

R #	Violation Severity Levels (CIP-006-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least 90 days. (Part 2.3)

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	4/16/2025	Approved by the Standards Committee	Errata

Version	Date	Action	Change Tracking
7.1	3/19/2026	FERC order issued approving CIP-006-7.1 Docket No. RM24-8-000	

Reliability Standard CIP-007-7.1

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

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

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process:

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

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

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

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

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

1.4. Additional Compliance Information:
None

Violation Severity Levels

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

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

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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

Version History

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

Version	Date	Action	Change Tracking
			impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	4/16/2025	Approved by the Standards Committee	Errata
7.1	3/19/2026	FERC order issued approving CIP-007-7.1. Docket No. RM24-8-000	

Reliability Standard CIP-008-7.1

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7.1

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7.1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7.1 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7.1 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated EACMS	No later than 60 calendar days after a change to the roles or responsibilities,	Examples of evidence may include, but are not limited to:

CIP-008-7.1 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7.1 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: •Roles or responsibilities, or •Cyber Security Incident response groups or individuals, or •Technology changes. (Part 3.2)	calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: •Roles or responsibilities, or •Cyber Security Incident response groups or individuals, or •Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column. (Requirement R4)	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Version	Date	Action	Change Tracking
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	4/16/2025	Approved by the Standards Committee	Errata
7.1	3/19/2026	FERC order issued approving CIP-008-7.1. Docket No. RM24-8-000	

Reliability Standard CIP-009-7.1

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7.1

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7.1:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7.1 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7.1 Table R1 – Recovery Plan Specifications*.

CIP-009-7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

CIP-009-7.1 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g., sample tape load, browsing tape contents) and compatibility with current system configurations (e.g., manual, or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7.1 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and

CIP-009-7.1 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 15 calendar months, not exceeding 16 calendar	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2)	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar months, not exceeding 18 calendar	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan(s)

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
7.1	4/16/2025	Approved by the Standards Committee	Errata

Version	Date	Action	Change Tracking
7.1	3/19/2026	FERC order issued approving CIP-009-7.1. Docket No. RM24-8-000	

Reliability Standard CIP-010-5

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

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

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required	The Responsible Entity neither documented nor implemented a configuration monitoring process(es); or the process does not include five or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	08/10/17	Adopted by the NERC Board of Trustees.	Modified to address certain directives in FERC Order No. 829.
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	11/05/2020	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 850.
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
5	5/9/2024	Approved by the NERC Board of Trustees.	Virtualization Modifications under Project 2016-02

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail,

policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Reliability Standard CIP-011-4.1

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4.1

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

   4.1.6 Transmission Operator

4.1.7 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

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

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

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

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

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

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4.1 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4.1 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4.1 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or

CIP-011-4.1 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		• Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011.1-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4.1 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4.1 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4.1)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4.1 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards. Responsible Entities

Version	Date	Action	Change Tracking
			must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	5/9/24	Adopted by the NERC Board of Trustees.	Virtualization Modifications
4.1	4/16/2025	Adopted by the Standards Committee	Errata
4.1	3/19/2026	FERC order issued approving CIP-011-4.1. Docket No. RM24-8-000	

Reliability Standard CIP-013-3

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

   4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in

this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

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

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

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

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

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

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

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

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	08/10/17	Adopted by the NERC Board of Trustees.	Respond to FERC Order No. 829.
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	11/05/2020	Adopted by the NERC Board of Trustees.	Modifications to address directive in FERC Order No. 850.
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
3	5/9/2024	Adopted by the NERC Board of Trustees	Virtualization Modifications by Project 2016-02

Reliability Standard BAL-007-1.1

A. Introduction

1. **Title:** Near-Term Energy Reliability Assessments
2. **Number:** BAL-007-1.1
3. **Purpose:** To assess, report, and plan to address forecasted Energy Emergencies in the near-term time horizon.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1.** Balancing Authority
5. **Effective Date:** See Implementation Plan for BAL-007-1.

B. Requirements and Measures

R1. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, document a process for conducting Near-Term Energy Reliability Assessments (ERA). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The Near-Term ERA process shall account for:

1.1.1. Forecasted or assumed Demand profiles;

1.1.2. Resource capabilities and operational limitations, including fuel supply;

1.1.3. Energy transfers with other Balancing Authorities; and

1.1.4. Known Bulk Electric System (BES) Transmission constraints that limit the ability of generation to deliver their output to Load.

1.2. The Near-Term ERA process shall specify the duration of the Balancing Authority's Near-Term ERAs.

1.3. The Near-Term ERA process shall specify the frequency at which the Balancing Authority will conduct Near-Term ERAs, subject to the following:

1.3.1. Each Balancing Authority will conduct Near-Term ERAs for all time periods unless the Balancing Authority demonstrates, via a documented methodology, that a Near-Term ERA is not necessary for a specified time period(s) because there is a low risk of an Energy Emergency occurring during that specified time period(s).

1.3.2. The documented methodology for identifying time periods for which the Balancing Authority will not conduct a Near-Term ERA must (i) define the criteria used to determine when there is a low risk of an Energy Emergency occurring, and (ii) account for the items listed in 1.1.1 – 1.1.4 and other conditions associated with Energy Emergencies.

M1. Each Balancing Authority shall have evidence that it documented a process for conducting Near-Term ERAs in accordance with Requirement R1.

R2. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, document a set of Scenarios, or a method for developing Scenarios, for use in performing Near-Term ERAs. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

2.1. The set of Scenarios must include (i) a base Scenario with expected system conditions, and (ii) other Scenarios that stress the system due to the following conditions, as applicable to the Balancing Authority's system:

2.1.1. Higher than forecasted or assumed Demand profiles;

2.1.2. The effects of an energy supply contingency;

2.1.3. The effects of a fuel supply contingency; and

2.1.4. Other stressed conditions that have a historical precedent of occurring, as defined by the Balancing Authority, based on the information available at the time of Scenario development.

M2. Each Balancing Authority shall have evidence that it documented the Scenarios, or the method of developing Scenarios, for use in performing Near-Term ERAs.

R3. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, document one or more Operating Plan(s) to implement in response to forecasted Energy Emergencies, including provisions for notification to their Reliability Coordinator of the forecasted Energy Emergency and the Operating Plan(s). *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Balancing Authority shall have evidence that it documented its Operating Plan(s) in accordance with Requirement R3.

R4. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, perform Near-Term ERAs according to the process documented in Requirement R1 using the Scenarios or methods documented in Requirement R2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Each Balancing Authority shall have evidence that it performed the Near-Term ERAs in accordance with Requirement R4.

R5. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, implement its Operating Plan(s), as documented in Requirement R3, when Near-Term ERAs identify any of the following forecasted Energy Emergencies: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- Forecasted EEA2 circumstances as defined in EOP-011 Attachment 1 Section B; or
- Forecasted EEA3 circumstances as defined in EOP-011 Attachment 1 Section B.

M5. Each Balancing Authority shall have evidence that it has implemented an Operating Plan(s) in accordance with Requirement R5.

R6. Each Balancing Authority shall, individually or jointly with other Balancing Authorities, review, update, as necessary, and provide to the applicable Reliability Coordinator its Near-Term ERA process, Scenarios or methods, and Operating Plan(s), documented under Requirements R1 through R3, at least once every 24 calendar months. *[Violation Risk Factor: Low] [Time Horizon: Operations Planning]*

M6. Each Balancing Authority shall have evidence that it reviewed and provided its Near-Term ERA process, Scenarios or methods, and Operating Plan(s) to its Reliability Coordinator, in accordance with Requirement R6.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

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

- The Balancing Authority shall keep data or evidence to show compliance with applicable requirements for six months for Near-Term ERAs or since the last audit.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Balancing Authority documented an Energy Reliability Assessment process for the Near-Term ERAs but did not account for the elements in Requirement R1 Part 1.1 or Part 1.2.	The Balancing Authority documented an Energy Reliability Assessment process for the Near-Term ERAs but did not account for the elements in Requirement R1 Part 1.1 through Part 1.2. OR The Balancing Authority documented an Energy Reliability Assessment process for the Near-Term ERAs but did not account for one of the elements in Requirement R1 Part 1.3.	The Balancing Authority failed to document an Energy Reliability Assessment process for the Near-Term ERAs. OR The Balancing Authority documented an Energy Reliability Assessment process for the Near-Term ERAs but did not account for any of the elements in Requirement R1 Part 1.3.
R2.	The Balancing Authority documented a set of Scenarios or a method of developing Scenarios but did not include one of the conditions listed in Requirement R2 Part 2.1.	The Balancing Authority documented a set of Scenarios or a method of developing Scenarios but did not include two of the conditions listed in Requirement R2 Part 2.1.	The Balancing Authority documented a set of Scenarios or a method of developing Scenarios but did not include three of the conditions listed in Requirement R2 Part 2.1.	The Balancing Authority documented a set of Scenarios or a method of developing Scenarios but did not include any of the conditions listed in Requirement R2 Part 2.1. OR The Balancing Authority failed to document a set of Scenarios or a method of developing Scenarios for use in performing Near-Term ERAs.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	N/A	N/A	The Balancing Authority documented an Operating Plan(s) to implement in response to forecasted Energy Emergencies as identified in the Near-Term ERAs but failed to include provisions for notification to the Reliability Coordinator.	The Balancing Authority failed to document an Operating Plan(s) to implement in response to forecasted Energy Emergencies as identified in the Near-Term ERAs.
R4.	N/A	N/A	N/A	The Balancing Authority failed to perform a Near-Term ERA in accordance with its process documented in Requirement R1 using the Scenarios or methods documented in Requirement R2.
R5.	N/A	N/A	N/A	The Balancing Authority failed to implement an Operating Plan(s) when a Near-Term ERA identified any of the forecasted conditions in Requirement R5.
R6.	N/A	N/A	The Balancing Authority reviewed information that contained the Near-Term ERAs process, the Scenarios or methods, and Operating Plan(s) but failed to update within 24 months.	The Balancing Authority failed to review, update, and provide the Near-Term ERAs process, the Scenarios or methods, and Operating Plan(s) to the Reliability Coordinator.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan
- NERC Project 2022-03 Technical Rationale
- NERC Project 2022-03 Project Page

Version History

Version	Date	Action	Change Tracking
1	December 10, 2024	Adopted by the NERC Board of Trustees	New standard under Project 2022-03
1	February 26, 2025	FERC Letter Order approving BAL-007-1. Docket No. RD25-5-000.	

Exhibit A-4

Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024

Exhibit A-4:
Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024

New Definitions	Effective Date
ACE Diversity Interchange	7/1/2025
Inadvertent Interchange Management (I_{IM})	7/1/2025
Revised Definitions	
Actual Net Interchange (NI_A)	7/1/2025
Area Control Error (ACE)	7/1/2025
Automatic Generation Control (AGC)	7/1/2025
Automatic Time Error Correction (ATEC)	7/1/2025
Balancing Authority Area (BAA)	7/1/2025
Balancing Contingency Event (BCE)	7/1/2025
Control Performance Standard (CPS)	7/1/2025
Disturbance	7/1/2025
Dynamic Interchange Schedule or Dynamic Schedule	7/1/2025
Frequency Bias Setting (FBS)	7/1/2025
Frequency Error	7/1/2025
Implemented Interchange	7/1/2025
Inadvertent Interchange	7/1/2025
Interchange Meter Error (I_{ME})	7/1/2025
Operating Reserve – Spinning	7/1/2025
Operating Reserve – Supplemental	7/1/2025
Overlap Regulation Service	7/1/2025
Pseudo-Tie	7/1/2025
Ramp Rate or Ramp	7/1/2025
Regulation Service	7/1/2025
Reportable Balancing Contingency Event (RBCE)	7/1/2025
Reporting Area Control Error (Reporting ACE)	7/1/2025
Reserve Sharing Group (RSG)	7/1/2025
Reserve Sharing Group Reporting ACE	7/1/2025
Scheduled Frequency	7/1/2025
Scheduled Net Interchange (NI_S)	7/1/2025
Supplemental Regulation Service	7/1/2025
Tie Line Bias (TLB)	7/1/2025
Time Error (TE)	7/1/2025
Time Error Correction (TEC)	7/1/2025

Exhibit A-5

Informational Summary of Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024

Exhibit A-5:
Informational Summary of Definitions Applicable to Nova Scotia, Approved by FERC in Second Quarter 2024

Reporting ACE Definition and Associated Terms	
Purpose	To improve the definition of Reporting Area Control Error (Reporting ACE), a term used in the Balancing and Control (BAL) family of Reliability Standards, to improve long-term average frequency performance as well as allow other Interconnections beyond the Western Interconnection the ability to pursue an automatic time error correction control methodology or similar functions.
Date of Petition and FERC Order	Petition filed on March 8, 2024, for approval of new and revised definitions of terms related to the calculation of Reporting Area Control Error or Reporting ACE with FERC in Docket No. RD24-6-000. FERC approved the Reliability Standard on April 29, 2024.

Exhibit A-6

Definitions Filed for Approval in Second Quarter 2024

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ACE Definition

Project 2022-01 Reporting ACE Definition and Associated Terms

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

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	Proposed New or Revised	Standards / Definitions Affected	Technical Guidelines / Reference Documents	Notes
Actual Net Interchange – (NI_A)	The algebraic sum of actual megawatt transfers across all Tie Lines, including Pseudo-Ties, to and from all Adjacent Balancing Authority areas within the same Interconnection. Actual megawatt transfers on asynchronous DC tie lines that are directly connected to another	The algebraic sum of actual megawatt transfers across all Tie Lines, including Pseudo-Ties, to and from all adjacent Balancing Authority Areas within the same Interconnection. Actual megawatt transfers on asynchronous DC tie lines that are directly connected to another	**Standards** • BAL-003-2 • BAL-004-WECC-3 **Terms** Reporting ACE (*current and proposed*)	Technical Reference Document: Balancing and Frequency Control Technical Reference Document: Integrating Reporting ACE with the NERC	Capitalized terms in definition.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Interconnection are excluded from Actual Net Interchange.	Interconnection are excluded from Actual Net Interchange.		Reliability Standards Technical Reference Document: Area Control Error Diversity Interchange Process Reliability Guideline: Inadvertent Interchange	
ACE Diversity Interchange (ADI)		A frequency neutral exchange program where multiple participating Balancing Authorities utilize it to achieve reductions in their generation control and Reporting ACE through offsets to either Actual Net Interchange or Scheduled Net Interchange ACE	Included in Reporting ACE definition.		New definition

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
		components to create an ACE value closer to zero for each participant.			
Area Control Error - (ACE)	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias, correction for meter error, and Automatic Time Error Correction (ATEC), if operating in the ATEC mode. ATEC is only applicable to Balancing Authorities in the Western Interconnection.	The instantaneous difference between an entity's Actual Net Interchange (NI_A) and Scheduled Net Interchange (NI_S), taking into account the effects of Frequency Bias, of correction for meter error, and of Inadvertent Interchange Management (I_{IM}) if operating in the I_{IM} mode. For compliance usage, refer to the term Reporting ACE.	**Standards** • BAL-002-3 (*purpose*) • BAL-003-2 • BAL-005-1 **Terms** • Control Performance Standard (*current; see proposed revisions*); • Disturbance Control Standard (*current; proposed for retirement*); • Frequency Bias	Reliability Guideline Operating Reserve Management Technical Reference Document: Balancing and Frequency Control Technical Reference Document: Area Control Error Diversity Interchange Process Inverter-Based Resource Performance Guideline	The old definition was restricted to only Balancing Authorities and excluded entities such as Balancing Authority Areas and Reserve Sharing Groups. Also updated terms to reflect current NERC defined terms and newly proposed terms added to the Reporting ACE term. Also added a clarifying statement to refer to Reporting ACE for compliance purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
			Setting (*current; see proposed revisions);* • Reporting ACE (*current and proposed*)		

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Automatic Time Error Correction – (ATEC)	The addition of a component to the ACE equation for the Western Interconnection that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange to correct accumulated time error. Automatic Time Error Correction is only applicable in the Western Interconnection. $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H}$ when operating in Automatic Time Error Correction Mode. The absolute value of I_{ATEC} shall not exceed L_{max} . I_{ATEC} shall be zero when operating in any other AGC mode.	The addition of a component , represented by the term $I_{ATEC,}$ to the Reporting ACE equation for the Western Interconnection that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange and to correct Time Error. Automatic Time Error Correction is only applicable in the Western Interconnection. $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H}$ The absolute value of I_{ATEC} shall not exceed $L_{Max.}$	**Standards** BAL-004-WECC-3 **Terms** Reporting ACE (*current and proposed*)	Technical Reference Document: Balancing Authority Area Footprint Change Tasks Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards Reliability Guideline: Inadvertent Interchange	Re-organized published glossary terms to reflect changes made during the standard drafting process. Published term was unreadable. Added an islanding term, "BA_{Island}" to accurately reflect a BA that has lost synchronism with the remainder of the interconnection cannot have an impact on Time Error. Changed the method of allocating Primary Inadvertent to use actual Bias settings to reflect each Balancing

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	• L_{max} is the maximum value allowed for $\mathbf{I_{ATEC}}$ set by each BA between $0.2*\lvert B_i\rvert$ and L_{10}, $0.2*\lvert B_i\rvert \leq L_{max} \leq L_{10}$ • $\mathbf{L_{10}} = 1.65 * \varepsilon_{10}\sqrt{(-10B_i)(-10B_S)}$ • $\boldsymbol{\varepsilon_{10}}$ is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-minute average frequency error based on frequency performance over a given year. The bound, ε 10, is the same for every Balancing Authority Area within an Interconnection. • $Y = B_i / B_S$.	I_{ATEC} shall be zero when operating in any other AGC mode. • L_{max} is the maximum value allowed for I_{ATEC} set by each BA between $0.2*\lvert B_i\rvert$ and L_{10}; i.e. $0.2*\lvert B_i\rvert \leq L_{max} \leq L_{10}$. • $L_{10} = 1.65 * \varepsilon_{10} * \sqrt{(-10B_i)(-10B_s)}$ • ε_{10} is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-minute average Frequency Error based on frequency performance over a given year. The bound, ε_{10}, is the same for every Balancing Authority Area within an Interconnection.			Authority's share of Time Error impact more accurately. Capitalized NERC defined terms.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	• H = Number of hours used to payback primary inadvertent interchange energy. The value of H is set to 3. • **B_i** = Frequency Bias Setting for the Balancing Authority Area (MW / 0.1 Hz). • B_S = Sum of the minimum Frequency Bias Settings for the Interconnection (MW / 0.1 Hz). • Primary Inadvertent Interchange (PII_{hourly}) is (1-Y) * (II_{actual} - B_i * ΔTE/6) • II_{actual} is the hourly Inadvertent Interchange for the last hour.	• Y = B_i/B_S. • H = Number of hours used to pay back primary Inadvertent Interchange energy. The value of H is set to 3. • B_i = Frequency Bias Setting for the Balancing Authority Area (MW/0.1 Hz). • B_s = Sum of the Frequency Bias Settings for the Interconnection (MW/0.1 Hz). For entities with a variable Frequency Bias, the annual time weighted average FBS based on the one minute values used in BAL-001 when frequency is greater than 60.036Hz or less than 59.964 Hz.			

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	• ΔTE is the hourly change in system Time Error as distributed by the Interconnection time monitor, where: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t)*(TE_{offset})$ • TD_{adj} is the Reliability Coordinator adjustment for differences with Interconnection time monitor control center clocks. • t is the number of minutes of manual Time Error Correction that occurred during the hour. • TE_{offset} is 0.000 or +0.020 or -0.020. • PII_{accum} is the Balancing Authority Area's accumulated PII_{hourly} in	• Primary Inadvertent Interchange (PII_{hourly}) is (1-Y) * ($II_{actual} - B_i$ * ΔTE/6) * BA_{Island} • BA_{Island} = Binary term: 1 indicates the BA is interconnected; 0 indicates the BA is entirely islanded and not interconnected. II_{actual} is the hourly Inadvertent Interchange for the last hour. • ΔTE is the hourly change in system Time Error as distributed by the Interconnection time monitor, where: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - t*(TE_{offset})$ • TD_{adj} is the Reliability Coordinator adjustment for differences with			

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	MWh. An On-Peak and Off-Peak accumulation accounting is required, where: $PII_{accum}^{on/offpeak} = last\ period's\ PII_{accum}^{on/offpeak} PII_{hourly}$	Interconnection time monitor control center clocks. • t is the number of minutes spent performing manual Time Error Correction that occurred during each hour. • TE_{offset} is 0.000 or +0.020 or -0.020. • PII_{accum} is the Balancing Authority Area's accumulated PII_{hourly} in MWh. An On-Peak and Off Peak accumulation accounting is required, where: $PII_{accum}^{on/offpeak} = last\ period's\ PII_{accum}^{on/offpeak} + PII_{hourly}$			
Balancing Authority Area (BAA)	The collection of generation, transmission, and loads within the metered boundaries of the	Added Acronym	**Standards** • BAL-003-2 • COM-001-3	Reliability Guideline: Operating Reserve Management	Added Acronym

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Balancing Authority. The Balancing Authority maintains load-resource balance within this area.		• EOP-004-4 • EOP-011-1 • MOD-004-1 • PRC-005-6 • TOP-001-5 **Terms** *Multiple terms*	Technical Reference Document: Balancing and Frequency Control Technical Reference Document: Balancing Authority Area Footprint Change Tasks Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	
Balancing Contingency	Any single event described in Subsections (A), (B), or	Any single event described in Subsections (A), (B), or	**Standards** BAL-002-3	Reliability Guideline	Added acronym and updated to

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Event – (BCE)	(C) below, or any series of such otherwise single events, with each separated from the next by one minute or less. A. Sudden loss of generation due to: i. unit tripping, or ii. loss of generator Facility resulting in isolation of the generator from the Bulk Electric System or from the responsible entity's System, or iii. sudden unplanned outage of transmission Facility; And, that causes an unexpected change to the responsible entity's ACE.	(C) below, or any series of such otherwise single events, with each separated from the next by one minute or less. A. Sudden loss of generation due to: i. unit tripping, or ii. loss of generator Facility resulting in isolation of the generator from the Bulk Electric System or from the responsible entity's System, or iii. sudden unplanned outage of transmission Facility; And, that causes an unexpected change to the responsible entity's Reporting ACE.	**Terms** • Contingency Reserve; • Most Severe Single Contingency; • Reportable Balancing Contingency Event	Operating Reserve Management Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards Technical Reference Document: Area Control Error Diversity Interchange Process	correct NERC defined term.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	B. Sudden loss of an Import, due to forced outage of transmission equipment that causes an unexpected imbalance between generation and Demand on the Interconnection. C. Sudden restoration of a Demand that was used as a resource that causes an unexpected change to the responsible entity's ACE.	B. Sudden loss of an import, due to forced outage of transmission equipment that causes an unexpected imbalance between generation and Demand on the Interconnection. C. Sudden restoration of a Demand that was used as a resource that causes an unexpected change to the responsible entity's Reporting ACE.			
Control Performance Standard – (CPS)	The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period.	Methodology of controlling Reporting ACE relative to Frequency Error, expressed as a moving average subject to a limit. It is used as an indicator of sufficient secondary AGC control to maintain energy balance	**Standards** • BAL-001-2 • BAL-003-2 (Attachment A) **Terms** None	Reliability Guideline: Operating Reserve Management Technical Reference Document:	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
		and Scheduled Frequency.		Balancing and Frequency Control Technical Reference Document: Area Control Error Diversity Interchange Process	
Disturbance	1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.	1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in Reporting ACE that is caused by the sudden failure of generation or interruption of load	**Standards** • BAL-002-3 • EOP-004-4 • EOP-005-3 • MOD-026-1 • MOD-027-1 • MOD-033-2 • PRC-026-1 **Terms** • Disturbance Control	Reliability Guideline: Operating Reserve Management Recommended Approaches for UFLS Program Design with Increasing Penetrations of DERs Methods for Establishing IROLs	Update to the NERC defined term “Reporting ACE” to accurately reflect current terminology.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
			Standard (*proposed for retirement)*; • Disturbance Monitoring Equipment	Reliability Guideline: Generating Unit Operations During Complete Loss of Communications Inverter-Based Resource Performance Guideline Reliability Guideline: Bulk Power System Reliability Perspectives on the Adoption of IEEE 1547-2018 Load Composition Guideline Reliability Guideline: Model Verification of Aggregate DER	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
				Models used in Planning Studies Power Plant Model Verification and Testing for Synchronous Machines DER Modeling Power Plant Model Verification for Inverter-Based Resources Reliability Guideline: DER Data Collection for Modeling in Transmission Planning Studies DER_A Model Parameterization Improvements to	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
				Interconnection Requirements for BPS-Connected Inverter-Based Resources	
Disturbance Control Standard – (DCS)	The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return its Area Control Error to within a specified range.	RETIRE	**Standards** BAL-002-3 **Terms** None	Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	RETIRE
Dynamic Interchange Schedule or Dynamic Schedule	A time-varying energy transfer that is updated in Real-time and included in the Scheduled Net Interchange (NIS) term in the same manner as an Interchange Schedule in the affected Balancing Authorities' control ACE equations (or alternate control processes).	A time-varying energy transfer that is updated in Real-time and included in the Scheduled Net Interchange (NI_S) term in the same manner as an Interchange Schedule in the affected Balancing Authorities' Reporting ACE .	**Standards** • BAL-002-WECC-3 • INT-009-3 **Terms** Scheduled Net Interchange (NI_S) (*current and proposed*)	Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	Update to the NERC defined term "Reporting ACE" to accurately reflect current terminology. Eliminated the word "equation" for consistency and eliminated the parenthetical which has no

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
					known application.
Frequency Bias Setting (FBS)	A number, either fixed or variable, usually expressed in MW/0.1 Hz, included in a Balancing Authority's Area Control Error equation to account for the Balancing Authority's inverse Frequency Response contribution to the Interconnection, and discourage response withdrawal through secondary control systems.	A negative number either fixed or variable, expressed in MW/0.1 Hz, included in a Balancing Authority's Reporting ACE to account for the Balancing Authority's Frequency Response to the Interconnection Frequency Error, and discourage response withdrawal through secondary control systems.	**Standards** • BAL-001-2 • BAL-003-2 **Terms** Reporting ACE (*current and proposed*)	Reliability Guideline: Operating Reserve Management Technical Reference Document: Balancing Authority Area Footprint Change Tasks Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	Added language to indicate this value must be a negative number and eliminated language to was not accepted in practice (usually). Update to the NERC defined term "Reporting ACE" to accurately reflect current terminology.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Frequency Error	The difference between the actual and scheduled frequency. ($F_A - F_S$)	The difference between the Actual Frequency and the Scheduled Frequency. ($F_A - F_S$)	**Standards:** • BAL-001-2 • MOD-027-1 **Term:** • Control Performance Standard • Reporting ACE • Frequency Regulation; • Reporting ACE (*current and proposed*); • Time Error Correction (*proposed*)	Power Plant Model Verification and Testing for Synchronous Machines DER_A Model Parameterization	
Inadvertent Interchange	The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled	The difference between the Balancing Authority's Actual Net Interchange and Scheduled Net Interchange.	**Standards** BAL-004-WECC-3 **Terms**	Technical Reference Document: Balancing and	Updated to correct NERC defined terms and correct acronyms.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Interchange. (IA – IS)	(NI_A – NI_S)	• Automatic Time Error Correction (I_{ATEC}) (*current and proposed*); • Dynamic Transfer; • Primary Inadvertent Interchange (WECC)	Frequency Control Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards Reliability Guideline: Inadvertent Interchange	
Inadvertent Interchange Management – (I_{IM})	New term to NERC glossary	A term used in Reporting ACE to allow for management of Inadvertent Interchange and correction of Time Error. The I_{IM} value is not used for unilateral paybacks and is null unless there is a regional procedure in place to	**Standards** None **Terms** Reporting Ace (*proposed*)		New term to NERC glossary

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
		coordinate an inadvertent control methodology for an Interconnection.			
Interchange Meter Error - (I_{ME})	A term used in the Reporting ACE calculation to compensate for data or equipment errors affecting any other components of the Reporting ACE calculation.	A term used in Reporting ACE to compensate for data or equipment errors affecting any other components of Reporting ACE.	**Standards** None **Terms** Reporting ACE (*current and proposed)*	Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	Eliminated the word "calculation" for consistency
Interchange Schedule	An agreed-upon Interchange Transaction size (megawatts), start and end time, beginning and ending ramp times and rate, and type required for delivery and receipt of power and energy between the Source and Sink Balancing Authorities involved in the transaction.	No changes	**Standards** MOD-028-2 **Terms** • Dynamic Interchange Schedule or Dynamic Schedule (*current and proposed*); • Net Interchange	Technical Reference Document: Balancing and Frequency Control Methods for Establishing IROLs	Team reviewed and determined no changes

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
			Schedule (*proposed for retirement*); • Net Scheduled Interchange (*proposed for retirement*); • Ramp Rate or Ramp (*see proposed revisions*); • Reliability Adjustment RFI; • Scheduling Entity; • Sink Balancing Authority; • Source Balancing Authority; • Tie Line Bias (*current and*		

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
			proposed)		
Implemented Interchange	The state where the Balancing Authority enters the Confirmed Interchange into its Area Control Error equation.	The state where the Balancing Authority enters the Confirmed Interchange into its Reporting ACE .	**Standards** None **Terms** • Reliability Adjustment; • Arranged Interchange		Update to the NERC defined term "Reporting ACE" to accurately reflect current terminology.
Net Interchange Schedule	The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.	Retire	**Standards** None **Terms** None	Reliability Guideline: Inadvertent Interchange	Retire. Term is no longer utilized.
Net Scheduled Interchange	The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time.	Retire	**Standards** None **Terms** None		Retire. Term is no longer utilized.
Operating Reserve – Spinning	The portion of Operating Reserve consisting of:	The portion of Operating Reserve consisting of:	**Standards** BAL-002-WECC-3	Reliability Guideline: Operating Reserve	Utilized proper capitalization on terms that are not

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	• Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.	• Generation synchronized to the system and fully available to serve load within the Disturbance recovery period following the contingency vent; or • Load fully removable from the system within the Disturbance recovery period following the contingency event.	**Terms** None	Management Technical Reference Document: Balancing and Frequency Control Power Plant Model Verification for Inverter-Based Resources	NERC defined.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Operating Reserve – Supplemental	The portion of Operating Reserve consisting of: • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.	The portion of Operating Reserve consisting of: • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance recovery period following the contingency event; or • Load fully removable from the system within the Disturbance recovery period following the contingency event.	**Standards** BAL-002-WECC-3 **Terms** None	Technical Reference Document: Balancing and Frequency Control Power Plant Model Verification for Inverter-Based Resources	Utilized proper capitalization on terms that are not NERC defined.
Overlap Regulation Service	A method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing	A method of providing Regulation Service in which the Balancing Authority providing the Regulation Service incorporates into its Reporting ACE a receiving Balancing Authority's	**Standards** • BAL-001-2 • BAL-003-2 **Terms** None	Technical Reference Document: Integrating Reporting ACE with the NERC Reliability	Update to the NERC defined term "Reporting ACE", "Actual Net Interchange", "Scheduled Net Interchange" and

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Authority's actual interchange, frequency response, and schedules into providing Balancing Authority's AGC/ACE equation.	Actual Net Interchange, Scheduled Net Interchange, and response to Interconnection Frequency Error.		Standards	"response to Interconnection Frequency Error", to accurately reflect current terminology.
Pre-Reporting Contingency Event ACE Value	The average value of Reporting ACE, or Reserve Sharing Group Reporting ACE when applicable, in the 16-second interval immediately prior to the start of the Contingency Event Recovery Period based on EMS scan rate data.	Team reviewed; no changes determined	**Standards** BAL-002-3 **Terms** None	Reliability Guideline: Operating Reserve Management	Update to the NERC defined term "Reporting ACE" to accurately reflect current terminology and grammatical changes to improve understanding.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Pseudo-Tie	A time-varying energy transfer that is updated in Real-time and included in the Actual Net Interchange term (NIA) in the same manner as a Tie Line in the affected Balancing Authorities' Reporting ACE equation (or alternate control processes).	A time-varying energy transfer that is updated in Real-time and included in the Actual Net Interchange term (NI_A) in the same manner as a Tie Line in the affected Balancing Authorities' Reporting ACE .	**Standards** • BAL-005-1 • BAL-002-WECC-3 • INT-009-3 **Terms** Actual Net Interchange (*current and proposed*)	Technical Reference Document: Balancing Authority Area Footprint Change Tasks	Eliminated the word "equation" for consistency and eliminated the parenthetical which has no known application.
Ramp Rate or Ramp	(Schedule) The rate, expressed in megawatts per minute, at which the interchange schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.	(Schedule) The rate, expressed in megawatts per minute, at which the Interchange Schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.	**Standards** None **Terms** Response Rate	Technical Reference Document: Balancing and Frequency Control Reliability Guideline: Generating Unit Operations During Complete Loss of Communications	Capitalized NERC defined terms within the definition.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
				Inverter-Based Resource Performance Guideline Performance, Modeling, and Simulations of BPS-Connected BESS and Hybrid Power Plants Reliability Guideline: Model Verification of Aggregate DER Models used in Planning Studies DER Modeling Power Plant Model Verification for Inverter-Based Resources Reliability	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
				Guideline: DER Data Collection for Modeling in Transmission Planning Studies DER_A Model Parameterization Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources	
Regulation Service	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the Reporting ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria	**Standards** • BAL-001-2 • BAL-003-2 **Terms** • Overlap Regulation Service (*proposed*);	Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	as specified by NERC for itself and the Balancing Authority for which it is providing the Regulation Service.	as specified by NERC for itself and the Balancing Authority for which it is providing the corrective response .	• Supplemental Regulation Service (*proposed*)		
Reporting Area Control Error – (Reporting ACE)	The scan rate values of a Balancing Authority Area's (BAA) Area Control Error (ACE) measured in MW includes the difference between the Balancing Authority Area's Actual Net Interchange and its Scheduled Net Interchange, plus its Frequency Bias Setting obligation, plus correction for any known meter error. In the Western Interconnection, Reporting ACE includes Automatic Time Error Correction($_{ATEC}$). Reporting ACE is calculated as follows: Reporting ACE = $(NI_A - NI_S) - 10B (F_A - F_S) - I_{ME}$	The scan rate values of a Balancing Authority Area's Area Control Error (ACE) measured in MW, which includes the error in scheduled interchange adjusted for Frequency Bias obligation, known meter error, and inadvertent management. Reporting ACE is calculated as follows: Reporting ACE = $(NI_A - NI_S) - 10B (F_A - F_S) - I_{ME} + I_{IM}$ Where: • NI_A = Actual Net Interchange. • NI_S = Scheduled Net Interchange.	**Standards** • BAL-001-2 • BAL-002-3 • BAL-005-1 **Terms** • Automatic Generation Control; • Interchange Meter Error (I_{ME}) *(current and proposed)*; • Pre-Reporting Contingency Event ACE Value; • Pseudo-Tie	Technical Reference Document: Balancing and Frequency Control Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards Technical Reference Document: Area Control Error Diversity Interchange	Modified to reflect a common term across all multiple BA interconnections. This change will allow regions to create methodologies to control Inadvertent Interchange accumulations.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Reporting ACE is calculated in the Western Interconnection as follows: Reporting ACE = $(NI_A - NI_S) - 10B (F_A - F_S) - I_{ME} + I_{ATEC}$ Where: • NI_A = Actual Net Interchange. • NI_S = Scheduled Net Interchange. • B = Frequency Bias Setting. • F_A = Actual Frequency. • F_S = Scheduled Frequency. • I_{ME} = Interchange Meter Error. • I_{IATEC} = Automatic Time Error Correction. All NERC Interconnections operate using the principles of Tie-line Bias	• B = Frequency Bias Setting. • F_A = Actual Frequency. • F_S = Scheduled Frequency. • I_{ME} = Interchange Meter Error. • I_{IM} = Inadvertent Interchange Management. (Term is expressed if a regional procedure exists, otherwise is null and is not included in the Balancing Authority's Reporting ACE.) o In the Western Interconnection this term is I_{ATEC} All NERC Interconnections operate using the principles of Tie Line Bias (TLB)	(*current and proposed*)	Process	

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	(TLB) Control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE equation that is(are) implemented for all BAAs on an Interconnection and is(are) consistent with the following four principles of Tie Line Bias control will provide a valid alternative to this Reporting ACE equation: 1. All portions of the Interconnection are included in exactly one BAA so that the sum of all BAAs' generation, load, and loss is the same as total Interconnection generation, load, and loss; 2. The algebraic sum of all BAAs' Scheduled Net Interchange is equal to	control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE that is(are) implemented for all BAAs in an Interconnection and is(are) consistent with the following four principles of Tie Line Bias control will provide a valid alternative to this Reporting ACE equation: 1. Each individual portion of the Interconnection is included in exactly one BAA so that the sum of all BAAs' generation, Load, and losses is the same as total Interconnection generation, Load, and losses; 2. The algebraic sum of all BAAs' Scheduled Net			

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	zero at all times and the sum of all BAAs' Actual Net Interchange values is equal to zero at all times; 3. The use of a common Scheduled Frequency FS for all BAAs at all times; and, 4. Excludes metering or computational errors. (The inclusion and use of the IME term corrects for known metering or computational errors.)	Interchange is equal to zero at all times and the sum of all BAAs' Actual Net Interchange values is equal to zero at all times. This includes effects of ACE Diversity Interchange (ADI) implementations; 3. The use of a common Scheduled Frequency for all BAAs at all times; and, 4. Excludes metering or computational errors. (The inclusion and use of the I_{ME} term corrects for known metering or computational errors.)			
Reportable Balancing Contingency Event – (RBCE)	Any Balancing Contingency Event occurring within a one-minute interval of an initial sudden decline in ACE based on EMS scan rate data that results in a loss of MW output less than or equal to the Most	Any Balancing Contingency Event occurring within a one-minute interval of an initial sudden decline in the responsible entity's Reporting ACE that results in a loss of MW output less than or equal to its Most	**Standards** BAL-002-3 **Terms** Contingency Event Recovery Period	Reliability Guideline: Operating Reserve Management Technical Reference Document: Area	Update to the NERC defined term "Reporting ACE" to accurately reflect current terminology. Moved note on modification of

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	Severe Single Contingency , and greater than or equal to the lesser amount of: (i) 80% of the Most Severe Single Contingency , or (ii) the amount listed below for the applicable Interconnection. Prior to any given calendar quarter, the 80% threshold may be reduced by the responsible entity upon written notification to the Regional Entity. • Eastern Interconnection – 900 MW • Western Interconnection – 500 MW • ERCOT – 800 MW • Quebec – 500 MW	Severe Single Contingency (MSSC) , and greater than or equal to the lesser amount of: (i) 80% of its MSSC. Prior to any given calendar quarter, the 80% threshold may be reduced by the responsible entity upon written notification to its Regional Entity, or (ii) the amount listed below for the applicable Interconnection. • Eastern Interconnection: 900 MW • Western Interconnection: 500 MW • ERCOT: 800 MW • Quebec: 500 MW		Control Error Diversity Interchange Process	80% threshold for readability.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Reportable Disturbance	Any event that causes ACE change greater than or equal to 80% of a Balancing Authority's or reserve sharing group's most severe contingency. The definition of a reportable disturbance is specified by each Regional Reliability Organization. This definition may not be retroactively adjusted in response to observed performance.	Retire	**Standards** CIP-002-5.1 (*outdated reference in G&TB*) **Terms** None		Retire
Reserve Sharing Group – (RSG)	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating reserves required for each Balancing Authority's use in recovering from contingencies within the	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply Operating Reserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy	**Standards** • PRC-005-6 • BAL-001-2 • BAL-002-3 • BAL-002-WECC-3 **Terms** Reserve Sharing	Reliability Guideline: Operating Reserve Management	Update to the NERC defined term "Operating Reserves" to accurately reflect current terminology. Replaced "disturbance control performance"

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in quicker (e.g., between zero and ten minutes) then, for the purposes of disturbance control performance, the areas become a Reserve Sharing Group.	from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in more quickly (e.g., between zero and ten minutes) then, for the purposes of recovery from a Reportable Balancing Contingency Event , the areas become a Reserve Sharing Group.	Group Reporting ACE		with "Balancing Contingency Event" to accurately reflect changes to BAL-002-3 terminology.
Reserve Sharing Group Reporting ACE	At any given time of measurement for the applicable Reserve Sharing Group (RSG), the algebraic sum of the ACEs (or equivalent as calculated at	At any given time of measurement for the applicable Reserve Sharing Group (RSG), the algebraic sum of the Reporting ACEs (or equivalent as calculated	**Standards** BAL-001-2 **Terms** None		Edited to accurately require a Reserve Sharing Group's Reporting ACE to use the sum of the Balancing

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	such time of measurement) of the Balancing Authorities participating in the RSG at the time of measurement.	at such time of measurement) of the Balancing Authorities participating in the RSG at the time of measurement.			Authorities Reporting ACE.
Scheduled Frequency	60.0 Hertz, except during a time correction	60.00 Hertz, except during a Time Error Correction	**Standards** • BAL-001-2 • MOD-027-1 **Terms** • Frequency Regulation; • Reporting ACE (*current and proposed*); • Time Error Correction (*proposed*)	Reliability Guideline: Operating Reserve Management Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards	Added resolution to the term as Time Error corrections are normally performed in +/- .02 Hz increments. Also capitalized terms that are NERC defined glossary terms.
Scheduled Net Interchange - (NI_S)	The algebraic sum of all scheduled megawatt transfers, including Dynamic Schedules, to and	Added acronym	**Standards** None **Terms**	Technical Reference Document: Balancing and	Added acronym

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	from all Adjacent Balancing Authority areas within the same Interconnection, including the effect of scheduled ramps. Scheduled megawatt transfers on asynchronous DC tie lines directly connected to another Interconnection are excluded from Scheduled Net Interchange.		Reporting ACE (*current and proposed*)	Frequency Control Technical Reference Document: Integrating Reporting ACE with the NERC Reliability Standards Technical Reference Document: Area Control Error Diversity Interchange Process Reliability Guideline: Inadvertent Interchange	
Supplemental Regulation Service	A method of providing regulation service in which the Balancing Authority	A method of providing Regulation Service in which the Balancing Authority	**Standards** None		Update to the NERC defined term “Reporting

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	providing the regulation service receives a signal representing all or a portion of the other Balancing Authority's ACE.	providing the Regulation Service receives a signal representing all or a portion of the other Balancing Authority's Reporting ACE.	**Terms** None		ACE" to accurately reflect current terminology.
Tie Line Bias (TLB)	A mode of Automatic Generation Control that allows the Balancing Authority to : 1) maintain its Interchange Schedule and 2) respond to Interconnection frequency error.	A mode of Automatic Generation Control that allows the Balancing Authority to : 1) maintain its Interchange Schedule and 2) respond to Interconnection Frequency Error.	**Standards** BAL-004-WECC-3 **Terms** Reporting ACE		Added acronym and capitalized defined terms.
Time Error (TE)	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. Time error is	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. The difference	**Standards** None **Terms** • Automatic Time Error Correction	Technical Reference Document: Balancing and Frequency Control Technical Reference	Added acronym commonly used and minor grammatical change to definition.

Table 1: Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
	caused by the accumulation of Frequency Error over a given period.	is caused by the accumulation of Frequency Error over a given period.	(*current and proposed*); • Time Error Correction (*current and proposed*)	Document: Integrating Reporting ACE with the NERC Reliability Standards	
Time Error Correction (TEC)	An offset to the Interconnection's scheduled frequency to return the Interconnection's Time Error to a predetermined value.	A manual offset to the Interconnection's Scheduled Frequency to return the Interconnection's Time Error to a predetermined range.	**Standards** BAL-004-WECC-3 **Terms** • Automatic Time Error Correction (*current and proposed*); • Scheduled Frequency (*proposed*)	Technical Reference Document: Balancing and Frequency Control Technical Reference Document: Balancing Authority Area Footprint Change Tasks	Added the word "manual" to indicate this process is not automatically implemented.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2022-01 Reporting ACE Definition and Associated Terms – Automatic Generation Control - (AGC) Errata| (Clean)

Retired, Modified, or Newly Proposed Definitions					
NERC Glossary Term	**Currently Approved Definition**	**Proposed New or Revised**	**Standards Effected / Definitions Affected**	**Technical Guidelines / Reference Documents**	**Notes**
Automatic Generation Control - (AGC)	A process designed and used to adjust a Balancing Authority Areas' Demand and resources to help maintain the Reporting ACE in that of a Balancing Authority Area within the bounds required by applicable NERC Reliability Standards.	A process designed and used to adjust a Balancing Authority Area's Demand and resources to help maintain the Reporting ACE in that Balancing Authority Area within the bounds required by applicable NERC Reliability Standards.	**Standards** BAL-004-WECC-3 **Terms** • Joint Control; • Regulating Reserve; • Tie Line Bias (*current and revised*)	Technical Reference Document: Balancing and Frequency Control Inverter-Based Resource Performance Guideline Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources	Team reviewed and determined minor grammar changes.

Exhibit B

List of Currently Effective NERC Reliability Standards

List of Currently Effective NERC Reliability Standards

BAL-001-2	Real Power Balancing Control Performance
BAL-001-TRE-2	Primary Frequency Response in the ERCOT Region
BAL-002-3	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event
BAL-002-WECC-3	Contingency Reserve
BAL-003-2	Frequency Response and Frequency Bias Setting
BAL-004-WECC-4	Automatic Time Error Correction
BAL-005-1	Balancing Authority Control
BAL-502-RF-03	Planning Resource Adequacy Analysis, Assessment and Documentation
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-9	Cyber Security — Security Management Controls
CIP-004-7	Cyber Security — Personnel & Training
CIP-005-7	Cyber Security — Electronic Security Perimeter(s)
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security — System Security Management
CIP-008-6	Cyber Security — Incident Reporting and Response Planning
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems
CIP-010-4	Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-011-3	Cyber Security — Information Protection
CIP-012-1	Cyber Security – Communications between Control Centers
CIP-013-2	Cyber Security - Supply Chain Risk Management
CIP-014-3	Physical Security
COM-001-3	Communications
COM-002-4	Operating Personnel Communications Protocols
EOP-004-4	Event Reporting
EOP-005-3	System Restoration from Blackstart Resources
EOP-006-3	System Restoration Coordination
EOP-008-2	Loss of Control Center Functionality
EOP-010-1	Geomagnetic Disturbance Operations
EOP-011-4	Emergency Operations
EOP-012-3	Extreme Cold Weather Preparedness and Operations
FAC-001-4	Facility Interconnection Requirements

FAC-002-4	Facility Interconnection Studies
FAC-003-5	Transmission Vegetation Management
FAC-008-5	Facility Ratings
FAC-011-4	System Operating Limits Methodology for the Operations Horizon
FAC-014-3	Establish and Communicate System Operating Limits
FAC-501-WECC-4	Transmission Maintenance
INT-006-5	Evaluation of Interchange Transactions
INT-009-3	Implementation of Interchange
IRO-001-4	Reliability Coordination – Responsibilities
IRO-002-7	Reliability Coordination – Monitoring and Analysis
IRO-006-5	Reliability Coordination — Transmission Loading Relief (TLR)
IRO-006-EAST-2	Transmission Loading Relief Procedure for the Eastern Interconnection
IRO-006-WECC-3	Qualified Path Unscheduled Flow (USF) Relief
IRO-008-3	Reliability Coordinator Operational Analyses and Real-time Assessments
IRO-009-2	Reliability Coordinator Actions to Operate Within IROLs
IRO-010-5	Reliability Coordinator Data and information Specification and Collection
IRO-014-3	Coordination Among Reliability Coordinators
IRO-017-1	Outage Coordination
IRO-018-1(i)	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities
MOD-025-2	Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability
MOD-026-2	Verification and Validation of Dynamic Models and Data
MOD-031-3	Demand and Energy Data
MOD-032-1	Data for Power System Modeling and Analysis
MOD-033-3	Steady-State and Dynamic System Model Validation
NUC-001-4	Nuclear Plant Interface Coordination
PER-003-2	Operating Personnel Credentials
PER-005-2	Operations Personnel Training
PER-006-1	Specific Training for Personnel
PRC-002-5	Disturbance Monitoring and Reporting Requirements
PRC-004-6	Protection System Misoperation Identification and Correction

PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance
PRC-006-5	Automatic Underfrequency Load Shedding
PRC-006-NPCC-2	Automatic Underfrequency Load Shedding
PRC-006-SERC-03	Automatic Underfrequency Load Shedding Requirements
PRC-008-0	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program
PRC-010-2	Undervoltage Load Shedding
PRC-011-0	Undervoltage Load Shedding System Maintenance and Testing
PRC-012-2	Remedial Action Schemes
PRC-017-1	Remedial Action Scheme Maintenance and Testing
PRC-019-2	Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection
PRC-023-6	Transmission Relay Loadability
PRC-024-3	Frequency and Voltage Protection Settings for Generating Resources
PRC-025-2	Generator Relay Loadability
PRC-026-2	Relay Performance During Stable Power Swings
PRC-027-1	Coordination of Protection Systems for Performance During Faults
PRC-028-1	Disturbance Monitoring and Reporting Requirements for Inverter-Based Resources
TOP-001-6	Transmission Operations
TOP-002-5	Operations Planning
TOP-003-6.1	Transmission Operator and Balancing Authority Data and Information Specification and Collection
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities
TPL-001-5.1	Transmission System Planning Performance Requirements
TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events
TPL-008-1	Transmission System Planning Performance Requirements for Extreme Temperature Events
VAR-001-5	Voltage and Reactive Control
VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules
VAR-501-WECC-4	Power System Stabilizer (PSS)

Exhibit C

Updated Glossary of Terms Used in NERC Reliability Standards

Glossary of Terms Used in NERC Reliability Standards

Updated April 1, 2026

This Glossary lists each term that was defined for use in one or more of NERC's continent-wide or Regional Reliability Standards and adopted by the NERC Board of Trustees from February 8, 2005, through April 1, 2026.

This reference is divided into the following sections:

Subject to Enforcement
Pending Enforcement
Filed and Pending Regulatory Approval
Regional Definitions

- **NPCC**
- **ReliabilityFirst**
- **Texas RE**
- **WECC**

Change History

The first three sections identify all terms that have been adopted by the NERC Board of Trustees for use in continent-wide standards; the Regional definitions section identifies all terms that have been adopted by the NERC Board of Trustees for use in regional standards.

Most of the terms identified in this glossary were adopted as part of the development of NERC's initial set of reliability standards, called the "Version 0" standards. Subsequent to the development of Version 0 standards, new definitions have been developed and approved per NERC's Reliability Standards Development Process, and added to this glossary following board adoption, FERC filing, and final Order approving the definition.

Any comments regarding this glossary should be reported to the NERC Help Desk. Select "Standards" from the "Service" drop-down menu and "Other" from the Standards Subcategory drop-down menu.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
ACE Diversity Interchange	Project-2022-01	ADI	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A frequency neutral exchange program where multiple participating Balancing Authorities utilize it to achieve reductions in their generation control and Reporting ACE through offsets to either Actual Net Interchange or Scheduled Net Interchange ACE components to create an ACE value closer to zero for each participant.
Actual Frequency (FA)	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	RM16-13-000	The Interconnection frequency measured in Hertz (Hz)
Actual Net Interchange	Project-2022-01	NI_A	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The algebraic sum of actual megawatt transfers across all Tie Lines, including Pseudo-Ties, to and from all adjacent Balancing Authority Areas within the same Interconnection. Actual megawatt transfers on asynchronous DC tie lines that are directly connected to another Interconnection are excluded from Actual Net Interchange.
Adequacy	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The ability of the electric system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.
Adjacent Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A Balancing Authority whose Balancing Authority Area is interconnected with another Balancing Authority Area either directly or via a multi-party agreement or transmission tariff.
Adverse Reliability Impact	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.
After the Fact	Project 2007-14	ATF	10/29/2008	12/17/2009	7/1/2010	RM09-8-000	A time classification assigned to an RFI when the submittal time is greater than one hour after the start time of the RFI.
Agreement	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A contract or arrangement, either written or verbal and sometimes enforceable by law.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Alternative Interpersonal Communication	Project 2006-06		11/7/2012	4/16/2015	10/1/2015	RM14-13-000	Any Interpersonal Communication that is able to serve as a substitute for, and does not utilize the same infrastructure (medium) as, Interpersonal Communication used for day-to-day operation.
Altitude Correction Factor	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A multiplier applied to specify distances, which adjusts the distances to account for the change in relative air density (RAD) due to altitude from the RAD used to determine the specified distance. Altitude correction factors apply to both minimum worker approach distances and to minimum vegetation clearance distances.
Ancillary Service	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Those services that are necessary to support the transmission of capacity and energy from resources to loads while maintaining reliable operation of the Transmission Service Provider's transmission system in accordance with good utility practice. (From FERC order 888-A.)
Anti-Aliasing Filter	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An analog filter installed at a metering point to remove the high frequency components of the signal over the AGC sample period.
Area Control Error	Project-2022-01	ACE	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The instantaneous difference between an entity’s Actual Net Interchange (NIA) and Scheduled Net Interchange (NIS), taking into account the effects of Frequency Bias, of correction for meter error, and of Inadvertent Interchange Management (IIM) if operating in the IIM mode. For compliance usage, refer to the term Reporting ACE.
Area Interchange Methodology	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	The Area Interchange methodology is characterized by determination of incremental transfer capability via simulation, from which Total Transfer Capability (TTC) can be mathematically derived. Capacity Benefit Margin, Transmission Reliability Margin, and Existing Transmission Commitments are subtracted from the TTC, and Postbacks and counterflows are added, to derive Available Transfer Capability. Under the Area Interchange Methodology, TTC results are generally reported on an area to area basis

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Arranged Interchange	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	The state where a Request for Interchange (initial or revised) has been submitted for approval.
Attaining Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A Balancing Authority bringing generation or load into its effective control boundaries through a Dynamic Transfer from the Native Balancing Authority.
Automatic Generation Control	Project-2022-01	AGC	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A process designed and used to adjust a Balancing Authority Area's Demand and resources to help maintain the Reporting ACE in that Balancing Authority Area within the bounds required by applicable NERC Reliability Standards.
Automatic Time Error Correction	Project-2022-01	ATEC	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The addition of a component , represented by the term IATEC, to the Reporting ACE equation for the Western Interconnection that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange and to correct Time Error. Automatic Time Erro Correction is only applicable in the Western InterconnectionIATEC shall be zero when operating in any other AGC mode. $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H}$ The absolute value of IATEC shall not exceed LMax. IATEC shall be zero when operating in any other AGC mode. • Lmax is the maximum value allowed for IATEC set by each BA between 0.2*|Bi| and L10; i.e. 0.2*|Bi|≤ Lmax ≤ L10. • $L_{10} = 1.65 * \varepsilon_{10} * \sqrt{(-10B_i)(-10B_s)}$

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							• ε10 is a constant derived from the targeted frequency bound. It is the targeted rootmean-square (RMS) valu of ten-minute average Frequency Error based on frequency performance over a given year. The bound, ε10, is the same for every Balancing Authority Area within an Interconnection. • Y = Bi/BS. • H = Number of hours used to pay back primary Inadvertent Interchange energy. The value of H is set to 3. • Bi = Frequency Bias Setting for the Balancing Authorit Area (MW/0.1 Hz). • Bs = Sum of the Frequency Bias Settings for the Interconnection (MW/0.1 Hz). For entities with a variable Frequency Bias, the annual time weighted average FBS based on the one minute values used in BAL-001 when frequency is greater than 60.036Hz or less than 59.964 Hz. • Primary Inadvertent Interchange (PII_{hourly}) is $(1-Y) * (II_{actual} - B_i * \Delta TE/6) * BA_{Island}$ • BAIsland = Binary term: 1 indicates the BA is interconnected; 0 indicates the BA is entirely islanded and not interconnected. IIactual is the hourly Inadvertent Interchange for the last hour. • ΔTE is the hourly change in system Time Error as distributed by the Interconnection time monitor, where: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - t*(TE_{offset})$ • TDadj is the Reliability Coordinator adjustment for

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							differences with Interconnection time monitor contro center clocks. • t is the number of minutes spent performing manual Time Error Correction that occurred during each hour • TEoffset is 0.000 or +0.020 or -0.020. • PIIaccum is the Balancing Authority Area's accumulated PIIhourly in MWh. An On-Peak and Off Peak accumulation accounting is required, where: $PII_{accum}^{on/offpeak} = last\ period's\ PII_{accum}^{on/offpeak} + PII_{hourly}$
Available Flowgate Capability	Project 2006-07	AFC	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A measure of the flow capability remaining on a Flowgate for further commercial activity over and above already committed uses. It is defined as TFC less Existing Transmission Commitments (ETC), less a Capacity Benefit Margin, less a Transmission Reliability Margin, plus Postbacks, and plus counterflows.
Available Transfer Capability	Project 2006-07	ATC	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. It is defined as Total Transfer Capability less Existing Transmission Commitments (including retail customer service), less a Capacity Benefit Margin, less a Transmission Reliability Margin, plus Postbacks, plus counterflows
Available Transfer Capability Implementation Document	Project 2006-07	ATCID	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A document that describes the implementation of a methodology for calculating ATC or AFC, and provides information related to a Transmission Service Provider's calculation of ATC or AFC.
Balancing Authority	Project 2010-14.2.1. Phase 2		2/11/2016	9/20/2017	1/1/2019	RM16-13-000	The responsible entity that integrates resource plans ahead of time, maintains Demand and resource balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Balancing Authority Area	Project-2022-01	BAA	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load-resource balance within this area.
Balancing Contingency Event	Project-2022-01	BCE	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	Any single event described in Subsections (A), (B), or (C) below, or any series of such otherwise single events, with each separated from the next by one minute or less. A. Sudden loss of generation due to: i. unit tripping, or ii. loss of generator Facility resulting in isolation of the generator from the Bulk Electric System or from the responsible entity's System, or iii. sudden unplanned outage of transmission Facility; And, that causes an unexpected change to the responsibl entity's Reporting ACE. B. Sudden loss of an import, due to forced outage of transmission equipment that causes an unexpected imbalance between generation and Demand on the Interconnection. C. Sudden restoration of a Demand that was used as a resource that causes an unexpected change to the responsible entity's Reporting ACE.
Base Load	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The minimum amount of electric power delivered or required over a given period at a constant rate.
BES Cyber Asset	Project 2014-02	BCA	2/12/2015	1/21/2016	7/1/2016	RM15-14-000	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
BES Cyber System Information	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
Blackstart Resource	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for Real and Reactive Power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Block Dispatch	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, the capacity of a given generator is segmented into loadable "blocks," each of which is grouped and ordered relative to other blocks (based on characteristics including, but not limited to, efficiency, run of river or fuel supply considerations, and/or "must-run" status).
Bulk Electric System	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014	RD14-2-000	(Please see the Implementation Plan for Phase 2 Compliance obligations.) Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. **Inclusions:** • **I1** - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded by application of Exclusion E1 or E3. • **I2** – Generating resource(s) including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above with: a) Gross individual nameplate rating greater than 20 MVA. Or, b) Gross plant/facility aggregate nameplate rating greater than 75 MVA. • **I3** - Blackstart Resources identified in the Transmission Operator's restoration plan. • **I4** - Dispersed power producing resources that aggregate to a total capacity greater than 75 MVA (gross nameplate rating), and that are connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage of 100 kV or above. Thus, the

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							facilities designated as BES are: a) The individual resources, and b) The system designed primarily for delivering capacity from the point where those resources aggregate to greater than 75 MVA to a common point of connection at a voltage of 100 kV or above. • **I5** –Static or dynamic devices (excluding generators) dedicated to supplying or absorbing Reactive Power that are connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, or through a transformer that is designated in Inclusion I1 unless excluded by application of Exclusion E4 **Exclusions:** • **E1** - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusions I2, I3, or I4, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or, c) Where the radial system serves Load and includes generation resources, not identified in Inclusions I2, I3 or I4, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating). Note 1 – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion. Note 2 – The presence of a contiguous loop, operated at a voltage level of 50 kV or less, between configurations being considered as radial systems, does not affect this exclusion.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							• **E2** - A generating unit or multiple generating units on the customer's side of the retail meter that serve all or part of the retail Load with electric energy if: (i) the net capacity provided to the BES does not exceed 75 MVA, and (ii) standby, back-up, and maintenance power services are provided to the generating unit or multiple generating units or to the retail Load by a Balancing Authority, or provided pursuant to a binding obligation with a Generator Owner or Generator Operator, or under terms approved by the applicable regulatory authority. • **E3** - Local networks (LN): A group of contiguous transmission Elements operated at less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN's emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customers and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following: a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusions I2, I3, or I4 and do not have an aggregate capacity of non-retail generation greater than 75 MVA (gross nameplate rating); b) Real Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and c) Not part of a Flowgate or transfer path: The LN does not contain any part of a permanent Flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection, or a comparable monitored Facility in the ERCOT or Quebec

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL). • **E4** – Reactive Power devices installed for the sole benefit of a retail customer(s). Note - Elements may be included or excluded on a case-by-case basis through the Rules of Procedure exception process.
Bulk-Power System	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms "Bulk-Power System" or "Bulk Power System" shall have the same meaning.)
Burden	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Operation of the Bulk Electric System that violates or is expected to violate a System Operating Limit or Interconnection Reliability Operating Limit in the Interconnection, or that violates any other NERC, Regional Reliability Organization, or local operating reliability standards or criteria.
Bus-tie Breaker	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	RM12-1-000	A circuit breaker that is positioned to connect two individual substation bus configurations.
Capacity Benefit Margin	000 - Version 0 Reliability Standards	CBM	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The amount of firm transmission transfer capability preserved by the transmission provider for Load-Serving Entities (LSEs), whose loads are located on that Transmission Service Provider's system, to enable access by the LSEs to generation from interconnected systems to meet generation reliability requirements. Preservation of CBM for an LSE allows that entity to reduce its installed generating capacity below that which may otherwise have been necessary without interconnections to meet its

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							generation reliability requirements. The transmission transfer capability preserved as CBM is intended to be used by the LSE only in times of emergency generation deficiencies.
Capacity Benefit Margin Implementation Document	Project 2006-07	CBMID	11/13/2008	11/24/2009	4/1/2011	RM08-19-000	A document that describes the implementation of a Capacity Benefit Margin methodology.
Capacity Emergency			2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A capacity emergency exists when a Balancing Authority Area's operating capacity, plus firm purchases from other systems, to the extent available or limited by transfer capability, is inadequate to meet its demand plus its regulating requirements.
Cascading	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The uncontrolled successive loss of System Elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.
CIP Exceptional Circumstance	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
CIP Senior Manager	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Clock Hour	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The 60-minute period ending at :00. All surveys, measurements, and reports are based on Clock Hour periods unless specifically noted.
Cogeneration	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Production of electricity from steam, heat, or other forms of energy produced as a by-product of another process.
Compliance Monitor	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The entity that monitors, reviews, and ensures compliance of responsible entities with reliability standards.
Composite Confirmed Interchange	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	The energy profile (including non-default ramp) throughout a given time period, based on the aggregate of all Confirmed Interchange occurring in that time period.
Composite Protection System	Project 2010-05.1		8/14/2014	5/13/2015	7/1/2016	RD14-14-000	The total complement of Protection System(s) that function collectively to protect an Element. Backup protection provided by a different Element's Protection System(s) is excluded.
Confirmed Interchange	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	The state where no party has denied and all required parties have approved the Arranged Interchange.
Congestion Management Report	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A report that the Interchange Distribution Calculator issues when a Reliability Coordinator initiates the Transmission Loading Relief procedure. This report identifies the transactions and native and network load curtailments that must be initiated to achieve the loading relief requested by the initiating Reliability Coordinator.
Consequential Load Loss	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	RM12-1-000	All Load that is no longer served by the Transmission system as a result of Transmission Facilities being removed from service by a Protection System operation designed to isolate the fault.
Constrained Facility	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A transmission facility (line, transformer, breaker, etc.) that is approaching, is at, or is beyond its System Operating Limit or Interconnection Reliability Operating Limit.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Contact Path	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An agreed upon electrical path for the continuous flow of electrical power between the parties of an Interchange Transaction.
Contingency	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element.
Contingency Event Recovery Period	Project 2010-14.1		11/5/2015	1/19/2017	1/1/2018	RM16-7-000	A period that begins at the time that the resource output begins to decline within the first one- minute interval of a Reportable Balancing Contingency Event, and extends for fifteen minutes thereafter.
Contingency Reserve	Project 2010-14.1		11/5/2015	1/19/2017	1/1/2018	RM16-7-000	The provision of capacity that may be deployed by the Balancing Authority to respond to a Balancing Contingency Event and other contingency requirements (such as Energy Emergency Alerts as specified in the associated EOP standard). A Balancing Authority may include in its restoration of Contingency Reserve readiness to reduce Firm Demand and include it if, and only if, the Balancing Authority: • is experiencing a Reliability Coordinator declared Energy Emergency Alert level, and is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan. • is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan.
Contingency Reserve Restoration Period	Project 2010-14.1		11/5/2015	1/19/2017	1/1/2018	RM16-7-000	A period not exceeding 90 minutes following the end of the Contingency Event Recovery Period.
Control Center	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
Control Performance Standard	Project-2022-01	CPS	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	Methodology of controlling Reporting ACE relative to Frequency Error, expressed as a moving average subject to a limit. It is used as an indicator of sufficient secondary AGC control to maintain energy balance and Scheduled Frequency.
Corrective Action Plan	Phase III-IV Planning Standards		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A list of actions and an associated timetable for implementation to remedy a specific problem.
Cranking Path	Phase III-IV Planning Standards		5/2/2006	3/16/2007	6/18/2007	RM06-16-000	A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.
Curtailment	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.
Curtailment Threshold	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The minimum Transfer Distribution Factor which, if exceeded, will subject an Interchange Transaction to curtailment to relieve a transmission facility constraint.
Cyber Assets	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident	Project 2018-02		2/7/2019	6/20/2019	1/1/2021	RD19-3-000	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or • Disrupts or attempts to disrupt the operation of a BES Cyber System

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Delayed Fault Clearing	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007	7/1/2008	RM07-3-000	Fault clearing consistent with correct operation of a breaker failure protection system and its associated breakers, or of a backup protection system with an intentional time delay.
Demand	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1.The rate at which electric energy is delivered to or by a system or part of a system, generally expressed in kilowatts or megawatts, at a given instant or averaged over any designated interval of time. 2.The rate at which energy is being used by the customer.
Demand-Side Management	Project 2010-04	DSM	5/6/2014	2/19/2015	7/1/2016	RM14-12-000	All activities or programs undertaken by any applicable entity to achieve a reduction in Demand.
Dial-up Connectivity	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.
Direct Control Load Management	Project 2008-06	DCLM	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Demand-Side Management that is under the direct control of the system operator. DCLM may control the electric supply to individual appliances or equipment on customer premises. DCLM as defined here does not include Interruptible Demand.
Dispatch Order	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, each generator is ranked by priority.
Dispersed Load by Substations	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.
Distributed Energy Resource	Project 2022-02	DER	10/31/2025	2/19/2026	4/1/2026	RD26-1-000	A generator or energy storage technology connected to a distribution system that is capable of providing Real Power in non-isolated parallel operation with the Bulk-Power System, including one connected behind the meter of an end-use customer that is supplied from a distribution system.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Distribution Factor	000 - Version 0 Reliability Standards	DF	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The portion of an Interchange Transaction, typically expressed in per unit that flows across a transmission facility (Flowgate).
Distribution Provider	Project 2015-04	DP	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	Provides and operates the "wires" between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the distribution function at any voltage
Disturbance	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in Reporting ACE that is caused by the sudden failure of generation or interruption of load.
Disturbance Control Standard	000 - Version 0 Reliability Standards	DCS	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return its Area Control Error to within a specified range.
Disturbance Monitoring Equipment	Phase III-IV Planning Standards	DME	8/2/2006	3/16/2007	6/18/2007	RM06-16-000	Devices capable of monitoring and recording system data pertaining to a Disturbance. Such devices include the following categories of recorders* : • Sequence of event recorders which record equipment response to the event • Fault recorders, which record actual waveform data replicating the system primary voltages and currents. This may include protective relays. Dynamic Disturbance Recorders (DDRs), which record incidents that portray power system behavior during dynamic events such as low-frequency (0.1 Hz – 3 Hz) oscillations and abnormal frequency or voltage

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							excursions *Phasor Measurement Units and any other equipment that meets the functional requirements
Dynamic Interchange Schedule or Dynamic Schedule	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A time-varying energy transfer that is updated in Real-time and included in the Scheduled Net Interchange (NIS) term in the same manner as an Interchange Schedule in the affected Balancing Authorities' Reporting ACE
Dynamic Transfer	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The provision of the real-time monitoring, telemetering, computer software, hardware, communications, engineering, energy accounting (including inadvertent interchange), and administration required to electronically move all or a portion of the real energy services associated with a generator or load out of one Balancing Authority Area into another.
Economic Dispatch	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The allocation of demand to individual generating units on line to effect the most economical production of electricity.
Electrical Energy	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).
Electronic Access Control or Monitoring Systems	Project 2008-06	EACMS	11/26/2012	11/22/2013	7/1/2016	RM13-5-000	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.
Electronic Access Point	Project 2008-06	EAP	11/26/2012	11/22/2013	7/1/2016	RM13-5-000	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter	Project 2008-06	ESP	11/26/2012	11/22/2013	7/1/2016	RM13-5-000	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
Element	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							line. An Element may be comprised of one or more components.
Emergency or BES Emergency	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.
Emergency Rating	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The rating as defined by the equipment owner that specifies the level of electrical loading or output, usually expressed in megawatts (MW) or Mvar or other appropriate units, that a system, facility, or element can support, produce, or withstand for a finite period. The rating assumes acceptable loss of equipment life or other physical or safety limitations for the equipment involved.
Emergency Request for Interchange	Project 2007-14	Emergency RFI	10/29/2008	12/17/2009	7/1/2010	RM09-8-000	Request for Interchange to be initiated for Emergency or Energy Emergency conditions.
Energy Emergency	000 - Version 0 Reliability Standards		11/13/2014	11/19/2015	4/1/2017	RM06-16-000	A condition when a Load-Serving Entity or Balancing Authority has exhausted all other resource options and can no longer meet its expected Load obligations.
Equipment Rating	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007	7/1/2008	RM07-3-000	The maximum and minimum voltage, current, frequency, real and reactive power flows on individual equipment under steady state, short-circuit and transient conditions, as permitted or assigned by the equipment owner.
Existing Transmission Commitments	Project 2006-07	ETC	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	Committed uses of a Transmission Service Provider's Transmission system considered when determining ATC or AFC.
External Routable Connectivity	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Extreme Cold Weather Temperature	Project-2021-07		2/15/2024	6/27/2024	10/1/2024	RD24-5-000	The temperature equal to the lowest 0.2 percentile of the hourly temperatures measured in December, January, and February from 1/1/2000 through the date the temperature is calculated.
Extreme Temperature Assessment	Project 2023-07		12/10/2024	2/20/2025	4/1/2026	RD25-4-000	Documented evaluation of future Bulk Electric System performance for extreme heat and extreme cold benchmark temperature events.
Facility	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007	7/1/2008	RM07-3-000	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.)
Facility Rating	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The maximum or minimum voltage, current, frequency, or real or reactive power flow through a facility that does not violate the applicable equipment rating of any equipment comprising the facility.
Fault	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection.
Fire Risk	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	The likelihood that a fire will ignite or spread in a particular geographic area.
Firm Demand	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	That portion of the Demand that a power supplier is obligated to provide except when system reliability is threatened or during emergency conditions.
Firm Transmission Service	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The highest quality (priority) service offered to customers under a filed rate schedule that anticipates no planned interruption.
Fixed Fuel Supply Component	Project-2021-07		2/15/2024	6/27/2024	10/1/2024	RD24-5-000	Non-mobile equipment that supports the reliable delivery of fuel to the generating unit and under the control of the Generator Owner at a plant site. Gaseous, liquid, or solid fuel handling components that are installed on site as fixed parts of the fuel delivery system that are under the Generator Owner's control are included. Mobile equipment such as trains, bulldozers, or other equipment

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							that are not fixed in one location are excluded.
Flashover	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	An electrical discharge through air around or over the surface of insulation, between objects of different potential, caused by placing a voltage across the air space that results in the ionization of the air space.
Flowgate	Project 2006-07		2/10/2009	11/24/2009	4/1/2011	RM08-19-000	1.) A portion of the Transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions. 2.) A mathematical construct, comprised of one or more monitored transmission Facilities and optionally one or more contingency Facilities, used to analyze the impact of power flows upon the Bulk Electric System.
Flowgate Methodology	Project 2006-07		2/10/2009	11/24/2009	4/1/2011	RM08-19-000	The Flowgate methodology is characterized by identification of key Facilities as Flowgates. Total Flowgate Capabilities are determined based on Facility Ratings and voltage and stability limits. The impacts of Existing Transmission Commitments (ETCs) are determined by simulation. The impacts of ETC, Capacity Benefit Margin (CBM) and Transmission Reliability Margin (TRM) are subtracted from the Total Flowgate Capability, and Postbacks and counterflows are added, to determine the Available Flowgate Capability (AFC) value for that Flowgate. AFCs can be used to determine Available Transfer Capability (ATC).
Forced Outage	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1. The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons. 2. The condition in which the equipment is unavailable due to unanticipated failure.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Frequency Bias	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A value, usually expressed in megawatts per 0.1 Hertz (MW/0.1 Hz), associated with a Balancing Authority Area that approximates the Balancing Authority Area's response to Interconnection frequency error.
Frequency Bias Setting	Project-2022-01	FBS	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A negative number either fixed or variable, expressed in MW/0.1 Hz, included in a Balancing Authority's Reporting ACE to account for the Balancing Authority's Frequency Response to the Interconnection Frequency Error, and discourage response withdrawal through secondary control systems.
Frequency Deviation	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A change in Interconnection frequency.
Frequency Error	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The difference between the Actual Frequency and the Scheduled Frequency. (FA –FS)
Frequency Regulation	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The ability of a Balancing Authority to help the Interconnection maintain Scheduled Frequency. This assistance can include both turbine governor response and Automatic Generation Control.
Frequency Response	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	(Equipment) The ability of a system or elements of the system to react or respond to a change in system frequency. (System) The sum of the change in demand, plus the change in generation, divided by the change in frequency, expressed in megawatts per 0.1 Hertz (MW/0.1 Hz).
Frequency Response Measure	Project 2007-12	FRM	2/7/2013	1/16/2014	4/1/2015	RM13-11-000	The median of all the Frequency Response observations reported annually by Balancing Authorities or Frequency Response Sharing Groups for frequency events specified by the ERO. This will be calculated as MW/0.1Hz.
Frequency Response Obligation	Project 2007-12	FRO	2/7/2013	1/16/2014	4/1/2015	RM13-11-000	The Balancing Authority's share of the required Frequency Response needed for the reliable operation of an Interconnection. This will be calculated as MW/0.1Hz.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Frequency Response Sharing Group	Project 2007-12	FRSG	2/7/2013	1/16/2014	4/1/2015	RM13-11-000	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating resources required to jointly meet the sum of the Frequency Response Obligations of its members.
Generation Capability Import Requirement	Project 2006-07	GCIR	11/13/2008	11/24/2009	4/1/2011	RM08-19-000	The amount of generation capability from external sources identified by a Load-Serving Entity (LSE) or Resource Planner (RP) to meet its generation reliability or resource adequacy requirements as an alternative to internal resources.
Generator Cold Weather Critical Component	Project-2021-07		2/15/2024	6/27/2024	10/1/2024	RD24-5-000	Any generating unit component or system, or associated Fixed Fuel Supply Component, that is under the Generator Owner's control, and is susceptible to freezing issues, the occurrence of which would likely lead to a Generator Cold Weather Reliability Event. This definition excludes any component or system or associated Fixed Fuel Supply Component located inside a permanent building with a heating source that regularly maintains the space at a temperature above 32 degrees Fahrenheit (0 degrees Celsius).
Generator Cold Weather Constraint	Project 2024-03		4/4/2025	9/18/2025	10/1/2025	RD25-7-000	Any condition that would preclude a Generator Owner from implementing freeze protection measures on one or more Generator Cold Weather Critical Components. Freeze protection measures are not intended to be limited to optimum practices, methods, or technologies, but are also intended to include practices, methods, or technologies that would be expected to result in improved generating unit performance during cold temperatures.
Generator Cold Weather Reliability Event	Project-2021-07		2/15/2024	6/27/2024	10/1/2024	RD24-5-000	One of the following events for which the apparent cause(s) is due to freezing of equipment or impacts of freezing precipitation (e.g., sleet, snow, ice, and freezing rain) on equipment within the Generator Owner's control, and the dry bulb temperature at the time of the event was at or above the Extreme Cold Weather Temperature: (1) a forced derate of more than 10% of the total capacity of the

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							unit, but not less than 20 MWs for longer than four hours in duration; (2) a start-up failure where the unit fails to synchronize within a specified start-up time; or (3) a Forced Outage.
Generator Operator	Project 2024-01	GOP	8/14/2025	10/1/2025	1/1/2026	RD25-10-000	The entity that: 1) operates generating Facility(ies) and performs the functions of supplying energy and Interconnected Operations Services (Category 1 GOP); or 2) operates non-BES Inverter-Based Resources(s) that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV (Category 2 GOP).
Generator Owner	Project 2024-01	GO	8/14/2025	10/1/2025	1/1/2026	RD25-10-000	The entity that: 1) owns and maintains generating Facility(ies) (Category 1 GO); or 2) owns and maintains non-BES Inverter-Based Resource(s) that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV (Category 2 GO).
Generator Shift Factor	000 - Version 0 Reliability Standards	GSF	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A factor to be applied to a generator's expected change in output to determine the amount of flow contribution that change in output will impose on an identified transmission facility or Flowgate.
Generator-to-Load Distribution Factor	000 - Version 0 Reliability Standards	GLDF	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The algebraic sum of a Generator Shift Factor and a Load Shift Factor to determine the total impact of an Interchange Transaction on an identified transmission facility or Flowgate.
Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability	Project 2013-03	GMD	12/17/2014	9/22/2016	7/1/2017	RM15-11-000	Documented evaluation of potential susceptibility to voltage collapse, Cascading, or localized damage of equipment due to geomagnetic disturbances.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Assessment							
Host Balancing Authority	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1. A Balancing Authority that confirms and implements Interchange Transactions for a Purchasing Selling Entity that operates generation or serves customers directly within the Balancing Authority's metered boundaries. 2. The Balancing Authority within whose metered boundaries a jointly owned unit is physically located.
Hourly Value	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Data measured on a Clock Hour basis.
Implemented Interchange	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The state where the Balancing Authority enters the Confirmed Interchange into its Reporting ACE .
Inadvertent Interchange	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The difference between the Balancing Authority's Actual Net Interchange and Scheduled Net Interchange. (NIA – NIS)
Inadvertent Interchange Management	Project-2022-01	I_{IM}	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A term used in Reporting ACE to allow for management of Inadvertent Interchange and correction of Time Error. The IIM value is not used for unilateral paybacks and is null unless there is a regional procedure in place to coordinate an inadvertent control methodology for an Interconnection.
Independent Power Producer	000 - Version 0 Reliability Standards	IPP	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, cogenerators and small power producers and all other nonutility electricity producers, such as exempt wholesale generators, who sell electricity.
Institute of Electrical and Electronics Engineers, Inc.	Project 2007-07	IEEE	2/7/2006	3/16/2007	6/18/2007	RM06-16-000	

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Interactive Remote Access	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process
Interchange	Coordinate Interchange		5/2/2006	3/16/2007	6/18/2007	RM06-16-000	Energy transfers that cross Balancing Authority boundaries.
Interchange Authority	Project 2015-04	IA	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The responsible entity that authorizes the implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes.
Interchange Distribution Calculator	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The mechanism used by Reliability Coordinators in the Eastern Interconnection to calculate the distribution of Interchange Transactions over specific Flowgates. It includes a database of all Interchange Transactions and a matrix of the Distribution Factors for the Eastern Interconnection.
Interchange Meter Error	Project-2022-01	I_{ME}	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A term used in Reporting ACE to compensate for data or equipment errors affecting any other components of Reporting ACE.
Interchange Schedule	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	An agreed-upon Interchange Transaction size (megawatts), start and end time, beginning and ending ramp times and rate, and type required for delivery and receipt of power and energy between the Source and Sink Balancing Authorities involved in the transaction.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Interchange Transaction	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An agreement to transfer energy from a seller to a buyer that crosses one or more Balancing Authority Area boundaries.
Interchange Transaction Tag or Tag	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The details of an Interchange Transaction required for its physical implementation.
Interconnected Operations Service	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	A service (exclusive of basic energy and Transmission Services) that is required to support the Reliable Operation of interconnected Bulk Electric Systems.
Interconnection	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	A geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control. When capitalized, any one of the four major electric system networks in North America: Eastern, Western, ERCOT and Quebec.
Interconnection Reliability Operating Limit	Determine Facility Ratings, Operating Limits, and Transfer Capabilities	IROL	11/1/2006	12/27/2007	7/1/2008	RM07-3-000	A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.
Interconnection Reliability Operating Limit Tv	Determine Facility Ratings, Operating Limits, and Transfer Capabilities	IROL Tv	11/1/2006	12/27/2007	7/1/2008	RM07-3-000	The maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's Tv shall be less than or equal to 30 minutes.
Intermediate Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A Balancing Authority on the scheduling path of an Interchange Transaction other than the Source Balancing Authority and Sink Balancing Authority.
Intermediate System	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	RM13-5-000	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							located inside the Electronic Security Perimeter.
Interpersonal Communication	Project 2006-06		11/7/2012	4/16/2015	10/1/2015	RM14-13-000	Any medium that allows two or more individuals to interact, consult, or exchange information.
Interruptible Load or Interruptible Demand	000 - Version 0 Reliability Standards		11/1/2006	3/16/2007	6/18/2007	RM06-16-000	Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment.
Inverter-Based Resource	Project 2020-06	IBR	10/8/2024	2/20/2025	4/1/2025	RM15-11-000	A plant/facility consisting of individual devices that are capable of exporting Real Power through a power electronic interface(s) such as an inverter or converter, and that are operated together as a single resource at a common point of interconnection to the electric system. Examples include, but are not limited to, plants/facilities with solar photovoltaic (PV), Type 3 and Type 4 wind, battery energy storage system (BESS), and fuel cell devices.
Joint Control	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Automatic Generation Control of jointly owned units by two or more Balancing Authorities.
Limiting Element	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The element that is 1.)Either operating at its appropriate rating, or 2,) Would be following the limiting contingency. Thus, the Limiting Element establishes a system limit.
Load	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An end-use device or customer that receives power from the electric system.
Load Shift Factor	000 - Version 0 Reliability Standards	LSF	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A factor to be applied to a load's expected change in demand to determine the amount of flow contribution that change in demand will impose on an identified transmission facility or monitored Flowgate.
Load-Serving Entity	Project 2015-04	LSE	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	Secures energy and Transmission Service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Long-Term Transmission Planning Horizon	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	RM12-1-000	Transmission planning period that covers years six through ten or beyond when required to accommodate any known longer lead time projects that may take longer than ten years to complete.
Market Flow	Project 2006-08		11/4/2010	4/21/2011	7/1/2011	RM06-16-000	The total amount of power flowing across a specified Facility or set of Facilities due to a market dispatch of generation internal to the market to serve load internal to the market.
Minimum Vegetation Clearance Distance	Project 2007-07	MVCD	11/3/2011	3/21/2013	7/1/2014	RM06-16-000	The calculated minimum distance stated in feet (meters) to prevent flash-over between conductors and vegetation, for various altitudes and operating voltages.
Misoperation	Project 2010-05.1		8/14/2014	5/13/2015	7/1/2016	RD14-14-000	The failure of a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation: 1. **Failure to Trip – During Fault** – A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct. 2. **Failure to Trip – Other Than Fault** – A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct. 3. **Slow Trip – During Fault** – A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System. 4. **Slow Trip – Other Than Fault** – A Composite Protection

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							System operation that is slower than required for a non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation, if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System. 5. **Unnecessary Trip – During Fault** – An unnecessary Composite Protection System operation for a Fault condition on another Element. 6. **Unnecessary Trip – Other Than Fault** – An unnecessary Composite Protection System operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.
Model Validation	Project 2020-06		8/14/2025	2/19/2026	4/1/2026	RD26-3-000	The process of comparing simulation results with measurements to assess how closely a model's behavior matches the measured behavior.
Model Verification	Project 2020-06		8/14/2025	2/19/2026	4/1/2026	RD26-3-000	The process of confirming that model structure and parameter values are representative of the equipment or facility design and settings by reviewing equipment or facility design and settings documentation.
Most Severe Single Contingency	Project 2010-14.1	MSSC	11/5/2015	1/19/2017	1/1/2018	RM16-7-000	The Balancing Contingency Event, due to a single contingency identified using system models maintained within the Reserve Sharing Group (RSG) or a Balancing Authority's area that is not part of a Reserve Sharing Group, that would result in the greatest loss (measured in MW) of resource output used by the RSG or a Balancing Authority that is not participating as a member of a RSG at the time of the event to meet Firm Demand and export obligation (excluding export obligation for which Contingency Reserve obligations are being met by the Sink Balancing Authority).

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Native Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A Balancing Authority from which a portion of its physically interconnected generation and/or load is transferred from its effective control boundaries to the Attaining Balancing Authority through a Dynamic Transfer.
Native Load	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The end-use customers that the Load-Serving Entity is obligated to serve.
Near-Term Transmission Planning Horizon	Project 2010-10		1/24/2011	11/17/2011	4/1/2013	RM08-19-000	The transmission planning period that covers Year One through five.
Net Actual Interchange	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The algebraic sum of all metered interchange over all interconnections between two physically Adjacent Balancing Authority Areas.
Net Energy for Load	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Net Balancing Authority Area generation, plus energy received from other Balancing Authority Areas, less energy delivered to Balancing Authority Areas through interchange. It includes Balancing Authority Area losses but excludes energy required for storage at energy storage facilities.
Network Integration Transmission Service	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Service that allows an electric transmission customer to integrate, plan, economically dispatch and regulate its network reserves in a manner comparable to that in which the Transmission Owner serves Native Load customers.
Non-Consequential Load Loss	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	RM12-1-000	Non-Interruptible Load loss that does not include: (1) Consequential Load Loss, (2) the response of voltage sensitive Load, or (3) Load that is disconnected from the System by end- user equipment.
Non-Firm Transmission Service	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Transmission service that is reserved on an as-available basis and is subject to curtailment or interruption.
Non-Spinning Reserve	000 - Version 0 Reliability		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1. That generating reserve not connected to the system but capable of serving demand within a specified time.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
	Standards						2. Interruptible load that can be removed from the system in a specified time.
Normal Clearing	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007	7/1/2008	RM07-3-000	A protection system operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed protection systems.
Normal Rating	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The rating as defined by the equipment owner that specifies the level of electrical loading, usually expressed in megawatts (MW) or other appropriate units that a system, facility, or element can support or withstand through the daily demand cycles without loss of equipment life.
Nuclear Plant Generator Operator	Project 2009-08		5/2/2007	10/16/2008	3/30/2009	RM08-3-000	Any Generator Operator or Generator Owner that is a Nuclear Plant Licensee responsible for operation of a nuclear facility licensed to produce commercial power.
Nuclear Plant Interface Requirements	Project 2009-08	NPIRs	5/2/2007	10/16/2008	3/30/2009	RM08-3-000	The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by the Nuclear Plant Generator Operator and the applicable Transmission Entities.
Nuclear Plant Licensing Requirements	Project 2009-08	NPLRs	5/2/2007	10/16/2008	3/30/2009	RM08-3-000	Requirements included in the design basis of the nuclear plant and statutorily mandated for the operation of the plant, including nuclear power plant licensing requirements for: 1) Off-site power supply to enable safe shutdown of the plant during an electric system or plant event; and 2) Avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.
Nuclear Plant Off-site Power Supply (Off-site Power)	Project 2009-08		5/2/2007	10/16/2008	3/30/2009	RM08-3-000	The electric power supply provided from the electric system to the nuclear power plant distribution system as required per the nuclear power plant license.
Off-Peak	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of lower electrical demand.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
On-Peak	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of higher electrical demand.
Open Access Same Time Information Service	000 - Version 0 Reliability Standards	OASIS	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An electronic posting system that the Transmission Service Provider maintains for transmission access data and that allows all transmission customers to view the data simultaneously.
Open Access Transmission Tariff	000 - Version 0 Reliability Standards	OATT	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Electronic transmission tariff accepted by the U.S. Federal Energy Regulatory Commission requiring the Transmission Service Provider to furnish to all shippers with non-discriminating service comparable to that provided by Transmission Owners to themselves.
Operating Instruction	Project 2007-02		5/6/2014	4/16/2015	7/1/2016	RM14-13-000	A command by operating personnel responsible for the Real-time operation of the interconnected Bulk Electric System to change or preserve the state, status, output, or input of an Element of the Bulk Electric System or Facility of the Bulk Electric System. (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.)
Operating Plan	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company- specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan
Operating Procedure	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A document that identifies specific steps or tasks that should be taken by one or more specific operating positions to achieve specific operating goal(s). The steps in an Operating Procedure should be followed in the order in which they are presented, and should be performed by the position(s) identified. A document that lists the specific steps for a system operator to take in removing a

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							specific transmission line from service is an example of an Operating Procedure.
Operating Process	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon Real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.
Operating Reserve	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages and local area protection. It consists of spinning and non-spinning reserve.
Operating Reserve – Spinning	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The portion of Operating Reserve consisting of: • Generation synchronized to the system and fully available to serve load within the Disturbance recovery period following the contingency event; or • Load fully removable from the system within the Disturbance recovery period following the contingency event.
Operating Reserve – Supplemental	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The portion of Operating Reserve consisting of: • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.
Operating Voltage	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	The voltage level by which an electrical system is designated and to which certain operating characteristics of the system are related; also, the effective (root-mean-square) potential difference between any two conductors or between a conductor and the ground. The actual voltage of the circuit may vary somewhat above or below this

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							value.
Operational Planning Analysis	Project 2007-06.2	OPA	8/11/2016	6/7/2018	4/1/2021	RM16-22-000	An evaluation of projected system conditions to assess anticipated (pre Contingency) and potential (post Contingency) conditions for next day operations. The evaluation shall reflect applicable inputs including, but not limited to: load forecasts; generation output levels; Interchange; known Protection System and Remedial Action Scheme status or degradation, functions, and limitations; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations. (Operational Planning Analysis may be provided through internal systems or through third party services.)
Operations Support Personnel	Project 2010-01		2/6/2014	6/19/2014	7/1/2016	RD14-7-000	Individuals who perform current day or next day outage coordination or assessments, or who determine SOLs, IROLs, or operating nomograms,1 in direct support of Real-time operations of the Bulk Electric System.
Outage Transfer Distribution Factor	Project 2006-07	OTDF	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	In the post-contingency configuration of a system under study, the electric Power Transfer Distribution Factor (PTDF) with one or more system Facilities removed from service (outaged).
Overlap Regulation Service	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A method of providing Regulation Service in which the Balancing Authority providing the Regulation Service incorporates into its Reporting ACE a receiving Balancing Authority's Actual Net Interchange, Scheduled Net Interchange, and response to Interconnection Error Frequency.
Participation Factors	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A set of dispatch rules such that given a specific amount of load to serve, an approximate generation dispatch can be determined. To accomplish this, generators are assigned a percentage that they will contribute to serve load.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Peak Demand	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1. The highest hourly integrated Net Energy For Load within a Balancing Authority Area occurring within a given period (e.g., day, month, season, or year). 2. The highest instantaneous demand within the Balancing Authority Area.
Performance-Reset Period	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007	7/1/2008	RM07-3-000	The time period that the entity being assessed must operate without any violations to reset the level of non compliance to zero.
Physical Access Control Systems	Project 2008-06	PACS	11/26/2012	11/22/2013	7/1/2016	RM13-5-000	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter	Project 2008-06	PSP	11/26/2012	11/22/2013	7/1/2016	RM13-5-000	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Planning Assessment	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	RM12-1-000	Documented evaluation of future Transmission System performance and Corrective Action Plans to remedy identified deficiencies.
Planning Authority	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The responsible entity that coordinates and integrates transmission Facilities and service plans, resource plans, and Protection Systems.
Planning Coordinator	Project 2006-07	PC	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	See Planning Authority.
Point of Delivery	000 - Version 0 Reliability Standards	POD	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Point of Receipt	Project 2015-04	POR	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a generator delivers its output.
Point to Point Transmission Service	000 - Version 0 Reliability Standards	PTP	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The reservation and transmission of capacity and energy on either a firm or non-firm basis from the Point(s) of Receipt to the Point(s) of Delivery.
Power Transfer Distribution Factor	Project 2006-07	PTDF	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	In the pre-contingency configuration of a system under study, a measure of the responsiveness or change in electrical loadings on transmission system Facilities due to a change in electric power transfer from one area to another, expressed in percent (up to 100%) of the change in power transfer
Pre-Reporting Contingency Event ACE Value	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The average value of Reporting ACE, or Reserve Sharing Group Reporting ACE when applicable, in the 16-second interval immediately prior to the start of the Contingency Event Recovery Period based on EMS scan rate data.
Pro Forma Tariff	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Usually refers to the standard OATT and/or associated transmission rights mandated by the U.S. Federal Energy Regulatory Commission Order No. 888.
Protected Cyber Assets	Project 2014-02	PCA	2/12/2015	1/21/2016	7/1/2016	RM15-14-000	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.
Protection System	Project 2007-17		11/19/2010	2/3/2012	4/1/2013	RM13-7-000	• Protective relays which respond to electrical quantities, • Communications systems necessary for correct operation of protective functions • Voltage and current sensing devices providing inputs to protective relays, • Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							• Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.
Protection System Coordination Study	Project 2007-06		11/5/2015	6/7/2018	4/1/2021	RM16-22-000	An analysis to determine whether Protection Systems operate in the intended sequence during Faults.
Protection System Maintenance Program (PRC-005-6)	Project 2007-17.4	PSMP	11/5/2015	12/18/2015	1/1/2016	RD16-2-000	An ongoing program by which Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components are kept in working order and proper operation of malfunctioning Components is restored. A maintenance program for a specific Component includes one or more of the following activities: • Verify — Determine that the Component is functioning correctly. • Monitor — Observe the routine in service operation of the Component. • Test — Apply signals to a Component to observe functional performance or output behavior, or to diagnose problems. • Inspect — Examine for signs of Component failure, reduced performance or degradation. • Calibrate — Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.
Pseudo-Tie	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A time-varying energy transfer that is updated in Real-time and included in the Actual Net Interchange term (NIA) in the same manner as a Tie Line in the affected Balancing Authorities' Reporting ACE .
Purchasing-Selling Entity	000 - Version 0 Reliability Standards	PSE	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Ramp Rate or Ramp	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	(Schedule) The rate, expressed in megawatts per minute, at which the Interchange Schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.
Rated Electrical Operating Conditions	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	The specified or reasonably anticipated conditions under which the electrical system or an individual electrical circuit is intend/designed to operate
Rated System Path Methodology	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	The Rated System Path Methodology is characterized by an initial Total Transfer Capability (TTC), determined via simulation. Capacity Benefit Margin, Transmission Reliability Margin, and Existing Transmission Commitments are subtracted from TTC, and Postbacks and counterflows are added as applicable, to derive Available Transfer Capability. Under the Rated System Path Methodology, TTC results are generally reported as specific transmission path capabilities.
Rating	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The operational limits of a transmission system element under a set of specified conditions.
Reactive Power	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive Power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive Power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).
Real Power	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The portion of electricity that supplies energy to the Load.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Real-time	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)
Real-time Assessment	Project 2007-06.2	RTA	8/11/2016	6/8/2018	4/1/2021	RM16-22-000	An evaluation of system conditions using Real time data to assess existing (pre Contingency) and potential (post Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load; generation output levels; known Protection System and Remedial Action Scheme status or degradation, functions, and limitations; Transmission outages; generator outages; Interchange; Facility Ratings; and identified phase angle and equipment limitations. (Realtime Assessment may be provided through internal systems or through third party services.)
Receiving Balancing Authority	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The Balancing Authority importing the Interchange.
Regional Reliability Organization	000 - Version 0 Reliability Standards	RRO	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	1. An entity that ensures that a defined area of the Bulk Electric System is reliable, adequate and secure. 2. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor.
Regional Reliability Plan	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The plan that specifies the Reliability Coordinators and Balancing Authorities within the Regional Reliability Organization, and explains how reliability coordination will be accomplished.
Regulating Reserve	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.
Regulation Reserve Sharing Group	Project 2010-14.1		8/15/2013	4/16/2015	7/1/2016	RM16-7-000	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply the Regulating Reserve required for all member Balancing Authorities to use in meeting applicable regulating standards.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Regulation Service	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the Reporting ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria as specified by NERC for itself and the Balancing Authority for which it is providing the corrective response .
Reliability Adjustment Arranged Interchange	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A request to modify a Confirmed Interchange or Implemented Interchange for reliability purposes.
Reliability Adjustment RFI	Project 2007-14		10/29/2008	12/17/2009	7/1/2010	RM09-8-000	Request to modify an Implemented Interchange Schedule for reliability purposes.
Reliability Coordinator	Project 2015-04	RC	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity that is the highest level of authority who is responsible for the Reliable Operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
Reliability Coordinator Area	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The collection of generation, transmission, and loads within the boundaries of the Reliability Coordinator. Its boundary coincides with one or more Balancing Authority Areas.
Reliability Coordinator Information System	000 - Version 0 Reliability Standards	RCIS	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The system that Reliability Coordinators use to post messages and share operating information in real time.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Reliability Standard	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	A requirement, approved by the United States Federal Energy Regulatory Commission under Section 215 of the Federal Power Act, or approved or recognized by an applicable governmental authority in other jurisdictions, to provide for Reliable Operation of the Bulk- Power System. The term includes requirements for the operation of existing Bulk-Power System facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for Reliable Operation of the Bulk-Power System, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.
Reliable Operation	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	Operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.
Remedial Action Scheme	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	RD16-5-000	A scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and Mvar), tripping load, or reconfiguring a System(s). RAS accomplish objectives such as: • Meet requirements identified in the NERC Reliability Standards; • Maintain Bulk Electric System (BES) stability; • Maintain acceptable BES voltages; • Maintain acceptable BES power flows; • Limit the impact of Cascading or extreme events. The following do not individually constitute a RAS: a. Protection Systems installed for the purpose of detecting Faults on BES Elements and isolating the faulted Elements

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							b. Schemes for automatic underfrequency load shedding (UFLS) and automatic undervoltage load shedding (UVLS) comprised of only distributed relays c. Out-of-step tripping and power swing blocking d. Automatic reclosing schemes e. Schemes applied on an Element for non-Fault conditions, such as, but not limited to, generator loss-of- field, transformer top-oil temperature, overvoltage, or overload to protect the Element against damage by removing it from service f. Controllers that switch or regulate one or more of the following: series or shunt reactive devices, flexible alternating current transmission system (FACTS) devices, phase-shifting transformers, variable-frequency transformers, or tap-changing transformers; and, that are located at and monitor quantities solely at the same station as the Element being switched or regulated g. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device h. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched i. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open j. Schemes that provide anti-islanding protection (e.g., protect load from effects of being isolated with generation that may not be capable of maintaining acceptable frequency and voltage) k. Automatic sequences that proceed when manually initiated solely by a System Operator l. Modulation of HVdc or FACTS via supplementary controls, such as angle damping or frequency damping applied to damp local or inter-area oscillations

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities (e.g., currents or torsional oscillations) n. Generator controls such as, but not limited to, automatic generation control (AGC), generation excitation [e.g. automatic voltage regulation (AVR) and power system stabilizers(PSS)], fast valving, and speed governing
Removable Media	Project 2016-02		2/9/2017	4/19/2018	1/1/2020	RM24-8-000	Storage media that: 1. are not Cyber Assets, 2. are capable of transferring executable code, 3. can be used to store, copy, move, or access data, and 4. are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or Protected Cyber Asset associated with high or medium impact BES Cyber Systems Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Reportable Balancing Contingency Event	Project-2022-01	RBCE	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	Any Balancing Contingency Event occurring within a one-minute interval of an initial sudden decline in the responsible entity's Reporting ACE that results in a loss of MW output less than or equal to its Most Severe Single Contingency (MSSC) , and greater than or equal to the lesser amount of: (i) 80% of its MSSC. Prior to any given calendar quarter, the 80% threshold may be reduced by the responsible entity upon written notification to its Regional Entity, or (ii) the amount listed below for the applicable

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							Interconnection. • Eastern Interconnection: 900 MW • Western Interconnection: 500 MW • ERCOT: 800 MW • Quebec: 500 MW
Reportable Cyber Security Incident	Project 2018-02		2/7/2019	6/20/2019	1/1/2021	RD19-3-000	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System
Reporting Area Control Error	Project-2022-01	Reporting ACE	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The scan rate values of a Balancing Authority Area's Area Control Error (ACE) measured in MW, which includes the error in scheduled interchange adjusted for Frequency Bias obligation, known meter error, and inadvertent management. Reporting ACE is calculated as follows: Reporting ACE = $(NI_A - NI_S) - 10B (F_A - F_S) - I_{ME} + I_{IM}$ Where: • NI_A = Actual Net Interchange. • NI_S = Scheduled Net Interchange. • B = Frequency Bias Setting. • F_A = Actual Frequency. • F_S = Scheduled Frequency. • I_{ME} = Interchange Meter Error. • I_{IM} = Inadvertent Interchange Management. (Term is expressed if a regional procedure exists, otherwise is null and is not included in the Balancing Authority's Reporting ACE.) ○ In the Western Interconnection this term is I_{ATEC} All NERC Interconnections operate using the principles of Tie Line Bias (TLB) control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE that is(are)

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							implemented for all BAAs in an Interconnection and is(are) consistent with the following four principles of Tie Line Bias control will provide a valid alternative to this Reporting ACE equation: 1. Each individual portion of the Interconnection is included in exactly one BAA so that the sum of all BAAs' generation, Load, and losses is the same as total Interconnection generation, Load, and losses; 2. The algebraic sum of all BAAs' Scheduled Net Interchange is equal to zero at all times and the sum of all BAAs' Actual Net Interchange values is equal to zero at all times. This includes effects of ACE Diversity Interchange (ADI) implementations; 3. The use of a common Scheduled Frequency for all BAAs at all times; and, 4. Excludes metering or computational errors. (The inclusion and use of the I_{ME} term corrects for known metering or computational errors.)
Request for Interchange	Project 2008-12	RFI	2/6/2014	6/30/2014	10/1/2014	RD14-4-000	A collection of data as defined in the NAESB Business Practice Standards submitted for the purpose of implementing bilateral Interchange between Balancing Authorities or an energy transfer within a single Balancing Authority.
Reserve Sharing Group	Project-2022-01	RSG	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply Operating Reserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in more quickly (e.g., between zero and ten minutes) then, for the purposes of recovery from a Reportable Balancing

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
							Contingency Event , the areas become a Reserve Sharing Group.
Reserve Sharing Group Reporting ACE	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	At any given time of measurement for the applicable Reserve Sharing Group (RSG), the algebraic sum of the Reporting ACEs (or equivalent as calculated at such time of measurement) of the Balancing Authorities participating in the RSG the time of measurement
Resource Planner	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority area.
Response Rate	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The Ramp Rate that a generating unit can achieve under normal operating conditions expressed in megawatts per minute (MW/Min).
Right-of-Way	Project 2010-07	ROW	5/9/2012	3/21/2013	7/1/2014	RM12-16-000	The corridor of land under a transmission line(s) needed to operate the line(s). The width of the corridor is established by engineering or construction standards as documented in either construction documents, pre-2007 vegetation maintenance records, or by the blowout standard in effect when the line was built. The ROW width in no case exceeds the applicable Transmission Owner's or applicable Generator Owner's legal rights but may be less based on the aforementioned criteria
Scenario	Coordinate Operations		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	Possible event.
Schedule	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Scheduled Frequency	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	60.00 Hertz, except during a Time Error Correction
Scheduled Net Interchange	Project-2022-01	NI_S	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The algebraic sum of all scheduled megawatt transfers, including Dynamic Schedules, to and from all Adjacent Balancing Authority areas within the same Interconnection, including the effect of scheduled ramps. Scheduled megawatt transfers on asynchronous DC tie lines directly connected to another Interconnection are excluded from Scheduled Net Interchange.
Scheduling Entity	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An entity responsible for approving and implementing Interchange Schedules.
Scheduling Path	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.
Sending Balancing Authority	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The Balancing Authority exporting the Interchange.
Sink Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	The Balancing Authority in which the load (sink) is located for an Interchange Transaction and any resulting Interchange Schedule.
Source Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	RD14-4-000	The Balancing Authority in which the generation (source) is located for an Interchange Transaction and for any resulting Interchange Schedule.
Special Protection System (Remedial Action Scheme)	Project 2010-05.2	SPS	5/5/2016	6/23/2016	4/1/2017	RD16-5-000	See “Remedial Action Scheme”
Spinning Reserve	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Unloaded generation that is synchronized and ready to serve additional demand.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Stability	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances.
Stability Limit	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The maximum power flow possible through some particular point in the system while maintaining stability in the entire system or the part of the system to which the stability limit refers.
Supervisory Control and Data Acquisition	000 - Version 0 Reliability Standards	SCADA	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A system of remote control and telemetry used to monitor and control the transmission system.
Supplemental Regulation Service	Project-2022-01		2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A method of providing Regulation Service in which the Balancing Authority providing the Regulation Service receives a signal representing all or a portion of the other Balancing Authority's Reporting ACE.
Surge	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.
Sustained Outage	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	The deenergized condition of a transmission line resulting from a fault or disturbance following an unsuccessful automatic reclosing sequence and/or unsuccessful manual reclosing procedure.
System	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A combination of generation, transmission, and distribution components.
System Operating Limit	Project-2015-09		5/13/2021	3/4/2022	4/1/2024	RD22-2-000	All Facility Ratings, System Voltage Limits, and stability limits, applicable to specified System configurations, used in Bulk Electric System operations for monitoring and assessing pre- and post Contingency operating states.
System Operator	Project 2010-01		2/6/2014	6/19/2014	7/1/2016	RD14-7-000	An individual at a Control Center of a Balancing Authority, Transmission Operator, or Reliability Coordinator, who operates or directs the operation of the Bulk Electric System (BES) in Real-time.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
System Voltage Limit	Project-2015-09		5/13/2021	3/4/2022	4/1/2024	RD22-2-000	The maximum and minimum steady-state voltage limits (both normal and emergency) that provide for acceptable System performance.
Telemetering	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The process by which measurable electrical quantities from substations and generating stations are instantaneously transmitted to the control center, and by which operating commands from the control center are transmitted to the substations and generating stations.
Thermal Rating	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The maximum amount of electrical current that a transmission line or electrical facility can conduct over a specified time period before it sustains permanent damage by overheating or before it sags to the point that it violates public safety requirements.
Tie Line	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A circuit connecting two Balancing Authority Areas.
Tie Line Bias	Project-2022-01	TLB	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A mode of Automatic Generation Control that allows the Balancing Authority to 1.) maintain its Interchange Schedule and 2.) respond to Interconnection frequency error.
Time Error	Project-2022-01	TE	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. The difference is caused by the accumulation of Frequency Error over a given period.
Time Error Correction	Project-2022-01	TEC	2/15/2024	4/29/2024	7/1/2025	RD24-6-000	A manual offset to the Interconnection's Scheduled Frequency to return the Interconnection's Time Error to a predetermined range.
TLR (Transmission Loading Relief) Log (NERC added the spelled out term for TLR Log for clarification	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Report required to be filed after every TLR Level 2 or higher in a specified format. The NERC IDC prepares the report for review by the issuing Reliability Coordinator. After approval by the issuing Reliability Coordinator, the report is electronically filed in a public area of the NERC Web site.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
purposes.)							
Total Flowgate Capability	Project 2006-07	TFC	8/22/2008	11/24/2009	4/1/2011	RM08-19-000	The maximum flow capability on a Flowgate, is not to exceed its thermal rating, or in the case of a flowgate used to represent a specific operating constraint (such as a voltage or stability limit), is not to exceed the associated System Operating Limit.
Total Internal Demand	Project 2010-04		5/6/2014	2/19/2015	7/1/2016	RM14-12-000	The Demand of a metered system, which includes the Firm Demand, plus any controllable and dispatchable DSM Load and the Load due to the energy losses incurred within the boundary of the metered system.
Total Transfer Capability	000 - Version 0 Reliability Standards	TTC	2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The amount of electric power that can be moved or transferred reliably from one area to another area of the interconnected transmission systems by way of all transmission lines (or paths) between those areas under specified system conditions.
Transaction	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	See Interchange Transaction.
Transfer Capability	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from “Area A” to “Area B” is *not g* enerally equal to the transfer capability from “Area B” to “Area A.”
Transfer Distribution Factor	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	See Distribution Factor.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Transient Cyber Asset	Project 2016-02	TCA	2/9/2017	4/19/2018	1/1/2020	RM24-8-000	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Transmission	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.
Transmission Constraint	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	A limitation on one or more transmission elements that may be reached during normal or contingency system operations.
Transmission Customer	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	1. Any eligible customer (or its designated agent) that can or does execute a Transmission Service agreement or can or does receive Transmission Service. 2. Any of the following entities: Generator Owner, Load-Serving Entity, or Purchasing-Selling Entity.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Transmission Line	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	A system of structures, wires, insulators and associated hardware that carry electric energy from one point to another in an electric power system. Lines are operated at relatively high voltages varying from 69 kV up to 765 kV, and are capable of transmitting large quantities of electricity over long distances.
Transmission Operator	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission Facilities.
Transmission Operator Area	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	The collection of Transmission assets over which the Transmission Operator is responsible for operating.
Transmission Owner	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity that owns and maintains transmission Facilities.
Transmission Planner	Project 2015-04		11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority area.
Transmission Reliability Margin	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The amount of transmission transfer capability necessary to provide reasonable assurance that the interconnected transmission network will be secure. TRM accounts for the inherent uncertainty in system conditions and the need for operating flexibility to ensure reliable system operation as system conditions change.
Transmission Reliability Margin Implementation Document	Project 2006-07		8/22/2008	11/24/2009	4/1/2011	RM08-19-000	A document that describes the implementation of a Transmission Reliability Margin methodology, and provides information related to a Transmission Operator's calculation of TRM.
Transmission Service	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	Services provided to the Transmission Customer by the Transmission Service Provider to move energy from a Point of Receipt to a Point of Delivery.

Subject to Enforcement							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Filing/Order Docket Number**	**Definition**
Transmission Service Provider	Project 2015-04	TSP	11/5/2015	1/21/2016	7/1/2016	RD16-3-000	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable Transmission Service agreements.
Undervoltage Load Shedding Program	Project 2008-02	UVLS Program	11/13/2014	11/19/2015	4/1/2017	RD15-5-000	An automatic load shedding program, consisting of distributed relays and controls, used to mitigate undervoltage conditions impacting the Bulk Electric System (BES), leading to voltage instability, voltage collapse, or Cascading. Centrally controlled undervoltage-based load shedding is not included.
Vegetation	Project 2007-07		2/7/2006	3/16/2007	6/18/2007	RM06-16-000	All plant material, growing or not, living or dead.
Vegetation Inspection	Project 2010-07		5/9/2012	3/21/2013	7/1/2014	RM12-16-000	The systematic examination of vegetation conditions on a Right-of-Way and those vegetation conditions under the applicable Transmission Owner's or applicable Generator Owner's control that are likely to pose a hazard to the line(s) prior to the next planned maintenance or inspection. This may be combined with a general line inspection.
Wide Area	000 - Version 0 Reliability Standards		2/8/2005	3/16/2007	6/18/2007	RM06-16-000	The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits.
Year One	Project 2010-10		1/24/2011	11/17/2011	4/1/2013	RM08-19-000	The first twelve month period that a Planning Coordinator or a Transmission Planner is responsible for assessing. For an assessment started in a given calendar year, Year One includes the forecasted peak Load period for one of the following two calendar years. For example, if a Planning Assessment was started in 2011, then Year One includes the forecasted peak Load period for either 2012 or 2013

Pending Enforcement						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
BES Cyber Asset	Project 2016-02	BCA	5/9/2024	3/19/2026	7/1/2028	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System	Project 2016-02	BCS	5/9/2024	3/19/2026	7/1/2028	*Update to Acronym only* One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
BES Cyber System Information	Project 2016-02	BCSI	5/9/2024	3/19/2026	7/1/2028	Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.
CIP Senior Manager	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Cyber Security Standards.
Control Center	Project 2021-03		12/10/2024	3/19/2026	7/1/2028	One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. OR One or more facilities of a Transmission Owner that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated

Pending Enforcement						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
						data centers, and excluding field Cyber Assets used for telemetry.
Cyber Assets	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring Systems; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BCS.
Cyber System (New Definition)	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems	Project 2016-02	EACMS	5/9/2024	3/19/2026	7/1/2028	Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point	Project 2016-02	EAP	5/9/2024	3/19/2026	7/1/2028	An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.
Electronic Security Perimeter	Project 2016-02	ESP	5/9/2024	3/19/2026	7/1/2028	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Energy Reliability Assessment	Project 2022-03	ERA	12/10/2024	2/26/2025	10/1/2026	Assessment of the resources necessary to reliably supply the Electrical Energy required to serve Demand and to provide Operating Reserves for the Bulk Power System throughout the associated assessment period.
External Routable Connectivity	Project 2016-02	ERC	5/9/2024	3/19/2026	7/1/2028	The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.
Interactive Remote Access	Project 2016-02	IRA	5/9/2024	3/19/2026	7/1/2028	User-initiated electronic access by a person using a bidirectional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface.

Pending Enforcement						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
						Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication.
Intermediate System	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.
Management Interface (New Definition)	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Near-Term Energy Reliability Assessment	Project 2022-03		12/10/2024	2/26/2025	10/1/2026	An Energy Reliability Assessment with an assessment period that begins no later than two days after the operating day and has a minimum duration of five days and a maximum duration of six weeks.
Physical Access Control Systems	Project 2016-02	PACS	5/9/2024	3/19/2026	7/1/2028	Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter	Project 2016-02	PSP	5/9/2024	3/19/2026	7/1/2028	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset	Project 2016-02	PCA	5/9/2024	3/19/2026	7/1/2028	One or more Cyber Assets or Virtual Cyber Assets (VCA) that: • Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or • Share CPU resources or memory resources with any part of the BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
Removable Media	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.
Reportable Cyber	Project 2016-02		5/9/2024	3/19/2026	7/1/2028	A Cyber Security Incident that compromised or disrupted:

Pending Enforcement						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Security Incident						• A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • An Electronic Security Perimeter of a high or medium impact BCS; • An Electronic Access Control or Monitoring Systems of a high or medium impact BCS; or • Shared Cyber Infrastructure supporting a BCS.
Ride-through	Project 2020-02		10/8/2024	7/24/2025	10/1/2026	The plant/facility remains connected and continues to operate through voltage or frequency system disturbances.
Shared Cyber Infrastructure (New Definition)	Project 2016-02	SCI	5/9/2024	3/19/2026	7/1/2028	One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset	Project 2016-02	TCA	5/9/2024	3/19/2026	7/1/2028	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. Capable of transmitting or transferring executable code; 2. Not included in a BES Cyber System (BCS); 3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS; and 4. Connected for 30 consecutive calendar days or less: • On a network protected by an Electronic Security Perimeter containing high or medium impact BCS; or • Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a: ▪ BES Cyber Asset; ▪ Shared Cyber Infrastructure; or ▪ PCA associated with high or medium impact BCS. Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability

Pending Enforcement						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
						assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (New Definition)	Project 2016-02	VCA	5/9/2024	3/19/2026	7/1/2028	A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets

Filed and Pending Regulatory Approval						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition

NPCC Regional Definitions							
Regional Term	**Link to Implementation Plan**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Current Zero Time	PRC-002-NPCC-1 Implementation Plan		11/4/2010	10/20/2011	10/20/2013		The time of the final current zero on the last phase to interrupt.
Generating Plant	PRC-002-NPCC-1 Implementation Plan		11/4/2010	10/20/2011	10/20/2013		One or more generators at a single physical location whereby any single contingency can affect all the generators at that location.

ReliabilityFirst Regional Definitions							
Regional Term	**Link to Implementation Plan**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Resource Adequacy	BAL-502-RFC-02 Implementation Plan		8/5/2009	3/17/2011	5/23/2011		The ability of supply-side and demand-side resources to meet the aggregate electrical demand (including losses)
Net Internal Demand	BAL-502-RFC-02 Implementation Plan		8/5/2009	3/17/2011	5/23/2011		Total of all end-use customer demand and electric system losses within specified metered boundaries, less Direct Control Management and Interruptible Demand
Year One	BAL-502-RFC-02 Implementation Plan		8/5/2009	3/17/2011	5/23/2011		The planning year that begins with the upcoming annual Peak Period

Texas RE Regional Definitions							
Regional Term	**Link to Implementation Plan**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Frequency Measurable Event	BAL-001-TRE-1 Implementation Plan	FME	8/15/2013	1/16/2014	4/1/2014		An event that results in a Frequency Deviation, identified at the BA's sole discretion, and meeting one of the following conditions: i) a Frequency Deviation that has a pre-perturbation [the 16-second period of time before t(0)] average frequency to post-perturbation [the 32- second period of time starting 20 seconds after t(0)] average frequency absolute deviation greater than 100 mHz (the 100 mHz value may be adjusted by the BA to capture 30 to 40 events per year). Or ii) a cumulative change in generating unit/generating facility, DC tie and/or firm load pre-perturbation megawatt value to post-perturbation megawatt value absolute deviation greater than 550 MW (the 550 MW value may be adjusted by the BA to capture 30 to 40 events per year).
Governor			8/15/2013	1/16/2014	4/1/2014		The electronic, digital or mechanical device that implements Primary Frequency Response of generating units/generating facilities or other system elements.
Primary Frequency Response	BAL-001-TRE-1 Implementation Plan	PFR	8/15/2013	1/16/2014	4/1/2014		The immediate proportional increase or decrease in real power output provided by generating units/generating facilities and the natural real power dampening response provided by Load in response to system Frequency Deviations. This response is in the direction that stabilizes frequency.

WECC Regional Definitions							
Regional Term	**Link to Standards Under Development**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Automatic Generation Control*	WECC Regional Standards Under Development	AGC	3/12/2007	6/8/2007	7/1/2007		Means equipment that automatically adjusts a Control Area's generation from a central location to maintain its interchange schedule plus Frequency Bias.
Automatic Time Error Correction	WECC Regional Standards Under Development	ATEC	12/19/2012	10/16/2013	4/1/2014		The addition of a component to the ACE equation that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange to correct accumulated time error.
Commercial Operation	WECC Regional Standards Under Development		10/29/2008	4/21/2011	7/1/2011		Achievement of this designation indicates that the Generator Operator or Transmission Operator of the synchronous generator or synchronous condenser has received all approvals necessary for operation after completion of initial start-up testing.
Primary Inadvertent Interchange	WECC Regional Standards Under Development		3/26/2008	5/21/2009	7/1/2009		The component of area (n) inadvertent interchange caused by the regulating deficiencies of the area (n).
Qualified Path	WECC Regional Standards Under Development		2/7/2019	5/10/2019	10/1/2019		A transmission element, or group of transmission elements that has qualified for inclusion into the Western Interconnection Unscheduled Flow Mitigation Plan (WIUFMP).

Change History	
Date	**Action**
4/1/2026	Moved: Distributed Energy Resource, Extreme Temperature Assessment, Model Validation, and Model Verification to Subject to Enforcement
4/1/2026	Moved: 2016-02 CIP Virtualization Terms to Pending Enforcement
2/27/2026	Moved: Model Validation and Model Verification to Pending Enforcement
2/19/2026	Moved: Distributed Energy Resource to Pending Enforcement
2/17/2026	Moved: Newly effective Generator Operator and Generator Owner terms to Subject to Enforcement and the inactive versions to Retired Terms Removed: Retired Terms
11/5/2025	Added: Distributed Energy Resource, Model Validation, and Model Verification to Filed and Pending Regulatory Approval
10/1/2025	Added: Generator Operator and Generator Owner to Pending Enforcement
10/1/2025	Moved: Generator Cold Weather Constraint to Subject to Enforcement and retired version to appropriate section
7/24/2025	Moved Ride-through to Pending Enforcement
7/10/2025	Corrected: Reporting ACE definition Moved: All 2022-01 terms to Subject to Enforcement and retired terms to appropriate section
4/10/2025	Added: Generator Cold Weather Constraint to Filed and Pending Regulatory Approval
2/26/2025	Added: Control Center and Ride-through to Filed and Pending Regulatory Approval Moved: Energy Reliability Assessment, Extreme Temperature Assessment, and Near-Term Energy Reliability Assessment to Pending Enforcement
1/7/2025	Added: Extreme Temperature Assessment, Energy Reliability Assessment, and Near-Term Energy Reliability Assessment to Filed and Pending Regulatory Approval Moved: Inverter-Based Resource to Pending Enforcement
11/4/2024	Added: Inverter-Based Resource to Filed and Pending Regulatory Approval
11/4/2024	Moved: EOP-012-2 terms (Generator Cold Weather Critical Component, Fixed Fuel Supply Component, Generator Cold Weather Reliability Event, Generator Cold Weather Constraint) to Subject to Enforcement
8/27/2024	Added “Filed and Pending Regulatory Approval” Category and 2016-02 CIP Virtualization Terms
7/22/2024	Updated EOP-012-2 terms (Generator Cold Weather Critical Component, Fixed Fuel Supply Component, Generator Cold Weather Reliability Event, Generator Cold Weather Constraint) to Pending Enforcement
5/7/2024	Updated ACE Definition to Pending Enforcement 7/1/2024
4/1/2024	Moved; to Subject to Enforcement Tab: System Voltage Limit, System Operating Limit
12/1/2023	Added; Actual Frequency to Subject to Enforcement Tab
3/8/2023	Updated Effective Date to 10/1/2024 for: 1 Generator Cold Weather Critical Component 2 Extreme Cold Weather Temperature 3 Generator Cold Weather Reliability Event
12/21/2022	Updated; Generator Cold Weather Critical Component, Extreme Cold Weather Temperature, Generator Cold Weather Reliability Event
12/2/2022	Updated; Automatic Time Error Correction (ATEC)
3/29/2022	Added to Pending Enforcement System Voltage Limit and System Operating Limit
4/2/2021	Retired; moved to the Retired Terms Tab: Reportable Cyber Security Incident
3/31/2021	Retired; moved to the Retired Terms tab:

Change History	
Date	**Action**
3/15/2021	Moved; to Subject to Enforcement Tab Operational Planning Analysis (OPA) Protections System Coordination Study 3 Real-time Assessment (RTA)
1/4/2021	Effective; moved to Subject to Enforcement Tab: Cyber Security Incident
1/4/2021	Retired; moved to the Retired Terms Tab: Cyber Security Incident
10/8/2020	Retired; moved to the Retired Terms tab. Automatic Generation Control Balancing Authority 3 Pseudo-Tie
5/29/2020	Updated effective date for Operational Planning Analysis (OPA), Protections System Coordination Study and Real-time Assessment (RTA) to 4/21/2021 per FERC/s April 17th Order extending effective dates due to COVID-19
2/24/2020	Added inactive Date to Qualified Transfer Path Curtailment Event, Contributing Schedule, Qualified Controllable Device, Relief Requirement and Transfer Distribution Factor
1/2/2020	Effective; moved to the Subject to Enforcement tab: Definition of Transient Cyber Asset (TCA) 2 Definition of Removable Media
1/2/2020	Retired; moved to the Retired Terms tab. Low Impact BES Cyber System Electronic Access Point (LEAP) Low Impact External Routable Connectivity (LERC) Transient Cyber Asset (TCA) 4 Removable Media
8/12/2019	Added revised definitions of Cyber Security Incident and Reportable Cyber Security Incident to the Pending Enforcement tab.
5/10/2019	Added Inactive Date to Qualified Transfer Path. Added Qualified Path definition and Effective Date
3/8/2019	Moved "Automatic Generation Control " "Balancing Authority" and "Pseudo-tie" to Subject to Enforcement tab
7/3/2018	Updated effective date for Operational Planning Analysis (OPA), Protections System Coordination Study and Real-time Assessment (RTA).
6/12/2018	Added revised definitions of Transient Cyber Asset and Removable Media to the Pending Enforcement tab.
1/31/2018	Fixed truncated definition for Texas RE term Primary Frequency Response
1/2/2018	Moved to Subject to Enforcement: Balancing Contingency Event; Contingency Event Recovery Period; Contingency Reserve; Contingency Reserve Restoration Period; Most Severe Single Contingency; Pre-Reporting Contingency Event ACE Value; Reportable Balancing Contingency Event; Reserve Sharing Group Reporting ACE Moved to Retired tab: Contingency Reserve; Reserve Sharing Group Reporting ACE
10/6/2017	Added the Effective date of Automatic Generation Control Pseudo-Tie and Balancing Authority
8/1/2017	Moved to Subject to Enforcement: Reporting Ace, Actual Frequency, Actual Net Interchange, Schedule Net Interchange, Interchange Meter Error Automatic Time Error Correction
7/24/2017	Updated project link for definitions related to Project 2014-02, board adopted 2/12/15.
7/14/2017	Updated project link to Remedial Action Scheme with an effective date of 4/1/17; Removeable

Change History	
Date	**Action**
	Media link to project 2014-02.
7/3/2017	Moved 'Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability Assessment' to Subject to Enforcement
6/15/2017	Readded 'Governor' and 'Primary Frequency Response' to Texas RE
4/4/2017	Moved to Subject to Enforcement: Energy Emergency, Remedial Action Scheme, Special Protection System and Under3 Voltage Load Shedding Program Moved terms inactive 3/31/17 to Retired tab
3/16/2017	Removed Pending Inactive tab; not necessary
3/10/2017	Added Pending Inactive tab
2/7/2017	Added Effective Dates for: Balancing Contingency Event, Most Severe Single Contingency (MSSC), Reportable Balancing Contingency Event, Contingency Event Recovery Period, Contingency Reserve Restoration Period, Pre-Reporting Contingency Event ACE Value, Reserve Sharing Group Reporting ACE Contingency Reserve
1/25/2017	Removed WECC terms 'Non-Spinning Reserve' and 'Spinning Reserve' per FERC Order No 789 Docket No RM13-13-000
1/6/2017	Moved the following terms from Pending Enforcement to Subject to Enforcement: Operational Planning Analysis, Real-time Assessment (Revised Definition)
1/5/2017	Formatting of Glossary of Terms updated.
12/12/16	Updated: 'Adverse Reliability Impact' from Pending to Retired. NERC withdrew the related petition 3/18/2015
11/28/16	Updated ReliabilityFirst - Wind Generating Station term to inactive
9/28/16	Updated CIP v 5 standards effective date from 4/1/2016 to 7/1/2016 per FERC Order 822
8/17/16	Board Adopted: Operational Planning Analysis and Real-time Assessment
7/13/16	Updated color coding of terms retired 6/30/2016 based on the terms becoming effective 7/1/2016.
6/24/16	FERC approved: Actual Frequency Actual Net Interchange Scheduled Net
	Interchange (NIS), Interchange Meter Error (IME), and Automatic Time Error Correction (ATEC)
	Reporting ACE: status updated
6/21/16	Correction: Reserve Sharing Group Reporting ACE, and Contingency Reserve changed to 11/5/2015 Board adoption date status
4/1/16	Effective: BES Cyber Asset, BES Cyber System, BES Cyber System Information, CIP Exceptional Circumstance, CIP Senior Manager, Cyber Assets, Cyber Security Incident, Dial-up Connectivity, Electronic Access Control or Monitoring Systems, Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, Interactive Remote Access, Intermediate System, Physical Access Control Systems, Physical Security Perimeter
3/31/16	Inactive: Critical Assets, Critical Cyber Assets, Cyber Assets, Cyber Security Incident, Electronic Security Perimeter, Physical Security Perimeter