
**BEFORE THE
NOVA SCOTIA UTILITY AND REVIEW BOARD
OF THE PROVINCE OF NOVA SCOTIA**

**North American Electric Reliability)
Corporation)**

**FOURTH QUARTER 2021 APPLICATION
FOR APPROVAL OF RELIABILITY STANDARDS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION**

Lauren A. Perotti
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net

February 15, 2022

I.	NOTICE AND COMMUNICATIONS	3
II.	REQUEST FOR APPROVAL OF RELIABILITY STANDARDS	3
A.	BACKGROUND: NERC QUARTERLY FILING OF PROPOSED RELIABILITY STANDARDS	3
B.	OVERVIEW OF NERC RELIABILITY STANDARDS DEVELOPMENT PROCESS.....	5
C.	DESCRIPTION OF PROPOSED REVISED RELIABILITY STANDARDS, FOURTH QUARTER 2021 .	6
1.	CIP-004-7	7
2.	CIP-011-3	8
D.	CONCLUSION.....	9

Exhibit A	Exhibit A-1: Reliability Standards Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2021
	Exhibit A-2: Informational Summary of Each Reliability Standard Applicable to Nova Scotia, Approved by FERC in Fourth Quarter 2021
	Exhibit A-3: Reliability Standards Filed for Approval
Exhibit B	List of Currently Effective NERC Reliability Standards
Exhibit C	Updated <i>Glossary of Terms Used in NERC Reliability Standards</i>

**BEFORE THE
NOVA SCOTIA UTILITY AND REVIEW BOARD
OF THE PROVINCE OF NOVA SCOTIA**

**North American Electric Reliability)
Corporation)**

**FOURTH QUARTER 2021 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 Utility and Review Board (“NSUARB”) an application for approval of NERC Reliability Standards approved by the United States Federal Energy Regulatory Commission (“FERC”) during the fourth quarter of 2021 (from October 1, 2021 through December 31, 2021). NERC requests that the Reliability Standards approved by FERC in the fourth quarter of 2021 be made mandatory and enforceable for users, owners, and operators of the Bulk-Power System (“BPS”) within the Province of Nova Scotia.

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 fourth quarter of 2021 (**Exhibit A-1**); (ii) an informational summary of the Reliability Standards applicable to Nova Scotia that were approved by FERC in the fourth quarter of 2021, 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 fourth quarter of 2021 (**Exhibit A-3**); (iv) an updated list of the currently effective NERC Reliability Standards as

approved by FERC (**Exhibit B**); and (v) the associated updated *Glossary of Terms Used in NERC Reliability Standards* (“*NERC Glossary*”) (**Exhibit C**).¹

I. NOTICE AND COMMUNICATIONS

Notices and communications regarding this application may be addressed to:

Lauren Perotti
Senior Counsel
North American Electric Reliability
Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@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”),² NERC is certified by FERC as the Electric Reliability Organization (“ERO”) in the United States.³ 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

¹ 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 NSUARB in the present quarterly application and all previous applications should be considered for purposes of this application.

² 16 U.S.C. § 824o(f) (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).

³ *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh’g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on compliance*, 118 FERC ¶ 61,190, *order on reh’g*, 119 FERC ¶ 61,046 (2007), *aff’d sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

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

NERC entered into a Memorandum of Understanding ("MOU") with the NSUARB,⁴ and a separate MOU with Nova Scotia Power Inc. ("NSPI") and the Northeast Power Coordinating Council, Inc. ("NPCC"),⁵ 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 memorializes the relationship between NERC and the NSUARB 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.⁶ In that decision, the NSUARB approved a quarterly review process for considering new and amended NERC Reliability Standards and criteria⁷ and ordered that "applications will not be processed by the Board until [FERC] has approved or remanded the standards in the United

⁴ See Memorandum of Understanding between Nova Scotia Utility and Review Board and North American Electric Reliability Corporation (signed Dec. 22, 2006).

⁵ 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).

⁶ *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].

⁷ *Id.* at P 30.

States.”⁸ The NSUARB Decision also stated that NSUARB approval is not required for the Violation Risk Factors (“VRFs”) and Violation Severity Levels (“VSLs”) associated with proposed Reliability Standards, but the NSUARB noted that it will accept VRFs and VSLs as guidance.⁹

Based on the NSUARB Decision, NERC applications to the NSUARB 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 VRFs and VSLs 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 VRFs and VSLs associated with NERC Reliability Standards.¹⁰ 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 NSUARB or other interested parties upon request.¹¹

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

⁸ *Id.*

⁹ *Id.* at P 33.

¹⁰ NERC’s VRF Matrix and VSL Matrix are available at <https://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States>. See the left-hand side of webpage for downloadable documents.

¹¹ 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/FilingsOrders/us/Pages/NERCFilings2021.aspx>.

electricity stakeholder segments. Stakeholders, through a balloting process, approve the Reliability 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 accordance with Section 300 (Reliability Standards Development) and Appendix 3A (Standard Processes Manual) of its Rules of Procedure.¹² NERC's Reliability Standards development process has been approved by the American National Standards Institute as being open, inclusive, balanced, and fair. The *NERC Glossary*, most recently updated June 28, 2021, 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.

C. Description of Proposed Revised Reliability Standards, Fourth Quarter 2021

As provided in the table below, during the fourth quarter of 2021, FERC issued a letter order approving two standards: Reliability Standards CIP-004-7 (Cyber Security – Personnel & Training) and CIP-011-3 (Cyber Security – Information Protection).¹³ No other Reliability Standards or definitions applicable to Nova Scotia were approved during the fourth quarter of 2021.

Reliability Standards	Effective Date
Critical Infrastructure Protection (CIP) Standards	
CIP-004-7*	1/1/2024
CIP-011-3*	1/1/2024

* 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.

The revised Reliability Standards improve the reliability of the Bulk Electric System (“BES”) by clarifying the protections required regarding use of third-party solutions for BES

¹² The NERC *Rules of Procedure* are available at <https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>.

¹³ *N. Am. Elec. Reliability Corp.*, Docket No. RD21-6-000 (Dec. 7, 2021) (delegated letter order).

Cyber System Information (“BCSI”). As technology has evolved, third-party services, such as cloud services, have become a viable and safe option for storing BCSI. As a result, the revisions in Reliability Standards CIP-004-7 and CIP-011-3 allow Responsible Entities to leverage these protections within their control for third-party data storage and analysis systems. The Reliability Standards maintain the security objectives supported in previous versions while providing flexibility for Responsible Entities to leverage third-party data storage and analysis systems. This project was initiated due to the work of an informal team, in collaboration with the NERC Compliance Input Working Group,¹⁴ to review the use of encryption on BCSI and its impact on compliance with NERC Reliability Standards.

FERC approved the two BCSI Reliability Standards in an order dated December 7, 2021. Additionally, FERC approved the violation risk factors and violation severity levels for the standards, the retirement of the currently effective versions of the standards, and the associated implementation plan.

I. CIP-004-7

Reliability Standard CIP-004-7 addresses Cyber Security – Personnel & Training and contains six requirements. The purpose of Reliability Standard CIP-004-7 (Cyber Security – Personnel & Training) is “To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.” The proposed

¹⁴ The Compliance Input Working Group was a subgroup of the now-disbanded NERC Critical Infrastructure Protection Committee, a stakeholder technical committee.

version of the standard adds “access management” to the purpose statement, which is otherwise unchanged from the currently effective version.

The revisions in CIP-004-7 center on removing references to “designated storage locations” and focusing the requirements on provisioned access to the BCSI, not just on where it is stored. This change permits entities to implement file-level rights and permissions, such as policy-based credentials or encryption, to manage access to BCSI.

New Requirement R6 applies to high impact BES Cyber Systems; medium impact BES Cyber Systems with External Routable Connectivity; and Electronic Access Control or Monitoring Systems (“EACMS”) and Physical Access Control Systems (“PACS”) associated with these high and medium BES Cyber Systems. There are three new requirement parts within Requirement R6. Part 6.1 requires Responsible Entities to authorize provisioned electronic access and provisioned physical access to BCSI. Part 6.2 incorporates into the access management program the obligation, formerly in Requirement R4 Part 4.4, to verify individuals with provisioned access are still appropriate. Finally, Part 6.3 incorporates into the provisioned access program the obligation, formerly in Requirement R5 Part 5.3, to remove an individual’s ability to use provisioned access to BCSI for a termination action.

Finally, there are additional other minor clarifications to update the standard which are shown in redline in Exhibit A-3. These include removal of functional entities that are no longer registered with NERC and replacing the term “Special Protection System” with “Remedial Action Scheme,” consistent with revisions made in other NERC Reliability Standards.

2. CIP-011-3

Reliability Standard CIP-011-3 addresses information protection of BCSI and includes two requirements. The purpose of Reliability Standard CIP-011-3 (Cyber Security – Information

Protection) is “To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).” The only modification of the purpose from the previous version of the standard is the inclusion of the BCSI acronym.

Requirement R1 includes the only substantive modifications in CIP-011-3. The revised Requirement R1 requires Responsible Entities to implement a documented information protection program(s) that includes the applicable requirement parts. The changes are designed to clarify requirements regarding protecting and securely handling BCSI. Additionally, as in CIP-004-7, there are additional other minor clarifications to update the standard. These revisions are shown in redline in Exhibit A-3.

D. CONCLUSION

NERC respectfully requests that the NSUARB approve the revised Reliability Standards and the retirement of the currently effective version of the standards, as specified herein.

Respectfully submitted,

/s/ Lauren Perotti

Lauren Perotti
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
lauren.perotti@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 15, 2022

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A

Exhibit A-1

Reliability Standards Applicable to Nova Scotia,
Approved by FERC in Fourth Quarter 2021

Reliability Standards	Effective Date
Critical Infrastructure Protection (CIP) Standards	
CIP-004-7*	1/1/2024
CIP-011-3*	1/1/2024

* 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.

Exhibit A-2:

Informational Summary of Each Reliability Standard Applicable to
Nova Scotia, Approved by FERC in Fourth Quarter 2021

Reliability Standard CIP-004-7	
Purpose	To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.
Applicability	<ul style="list-style-type: none">• Balancing Authority• Distribution Provider• Generator Operator• Generator Owner• Reliability Coordinator• Transmission Operator• Transmission Owner
Requirements	Reliability Standard CIP-004-7 contains six requirements.
Date of Petition and FERC Order	Petition filed September 15, 2021 for approval of CIP-004-7 with FERC in Docket No. RD21-6-000. FERC approved the revised Reliability Standard on December 7, 2021.

Reliability Standard CIP-011-3	
Purpose	To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
Applicability	<ul style="list-style-type: none">• Balancing Authority• Distribution Provider• Generator Operator• Generator Owner• Reliability Coordinator• Transmission Operator• Transmission Owner
Requirements	Reliability Standard CIP-011-3 contains two requirements.
Date of Petition and FERC Order	Petition filed September 15, 2021 for approval of CIP-011-3 with FERC in Docket No. RD21-6-000. FERC approved the revised Reliability Standard on December 7, 2021.

Exhibit A-3

Reliability Standards Filed for Approval

Exhibit A-3

CIP-004-7
Clean

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-7
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1. **Balancing Authority**
 - 4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3. **Generator Operator**
 - 4.1.4. **Generator Owner**
 - 4.1.5. **Reliability Coordinator**

4.1.6. Transmission Operator**4.1.7. Transmission Owner**

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

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

4.2.1.1. Each UFLS or UVLS System that:

- 4.2.1.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.2.1.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

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

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

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

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

- 4.2.3. Exemptions:** The following are exempt from Standard CIP-004-7:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-004-7.

6. Background: Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

as an all-inclusive list.

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

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

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CS0706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

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

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	<p>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:</p> <ul style="list-style-type: none"> • 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-004-7 Table R2 – Cyber Security Training Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including 	<p>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.</p>

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
		Transient Cyber Assets, and with Removable Media.	
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to confirm identity.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.</p>
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 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 	<p>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.</p>

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
	2. PACS	<p>for six consecutive months or more.</p> <p>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.</p>	
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
	2. PACS		
3.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.</p>

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter 	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.</p>
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • 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 <p>Dated documentation of the</p>

CIP-004-7 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 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 <p>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.</p>

- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and <p>Logs or other demonstration showing such persons no longer have access.</p>
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form showing a review of logical and physical access; and <p>Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.</p>
5.3	High Impact BES Cyber Systems and their associated:	For termination actions, revoke the individual's non-shared user accounts	An example of evidence may include, but is not limited to, workflow or sign-

CIP-004-7 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
	<ul style="list-style-type: none"> EACMS 	(unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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.</p> <p>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.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> Workflow or sign-off form showing password reset within 30 calendar days of the termination; Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or <p>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.</p>

- 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-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 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-004-7 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-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>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:</p> <p>6.1.1. Provisioned electronic access to electronic BCSI; and</p> <p>6.1.2. Provisioned physical access to physical BCSI.</p>	<p>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.</p>

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:</p> <ol style="list-style-type: none"> 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. 	<p>Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following:</p> <ul style="list-style-type: none"> • 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	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.</p>	<p>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.</p>

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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	Operations Planning	Medium	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	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 (PRAs), for individuals, including contractors and service vendors, for obtaining and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did</p>	<p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did</p>	<p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did</p>	<p>retaining authorized cyber or authorized unescorted physical access. (R3)</p> <p>OR</p> <p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)</p>	<p>not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)</p>	<p>not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk</p>	<p>and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	<p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	Operations Planning and Same Day Operations	Medium	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within</p>	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct</p>	<p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct</p>	<p>The Responsible Entity did not implement any documented program(s) for access management. (R4)</p> <p>OR</p> <p>The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1)</p> <p>OR</p> <p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	Same Day Operations	Medium	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		<p>user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4)</p> <p>OR</p>	<p>unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of</p>	<p>unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of</p>	<p>revocation for electronic access or unescorted physical access. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</p> <p>OR</p> <p>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not</p>	<p>authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</p> <p>OR</p> <p>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did</p>	<p>authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</p> <p>OR</p> <p>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did</p>	<p>OR</p> <p>The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</p> <p>OR</p> <p>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3	12/16/09	<p>Updated Version Number from -2 to -3</p> <p>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.</p>	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSl.

Exhibit A-3

CIP-004-7
Redline

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~76~~
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, ~~and~~ security awareness, and access management in support of protecting BES Cyber Systems.

4. Applicability:

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

4.1.1. Balancing Authority

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

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

- 4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.4.1.5.~~ Reliability Coordinator

~~4.1.7.4.1.6.~~ Transmission Operator

~~4.1.8.4.1.7.~~ Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

- 4.2.1.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- 4.2.1.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~76~~:

- 4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.3.3.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- 4.2.3.4.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

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

5. **Effective Dates:** See Implementation Plan for CIP-004-76.

6. **Background:**

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

“Applicable Systems” Columns in Tables:

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

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

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-~~76~~ 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-~~76~~ Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- 76 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	<p>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:</p> <ul style="list-style-type: none"> • 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-~~76~~ 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-~~76~~ Table R2 – *Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~76~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. 	<p>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.</p>

CIP-004-~~76~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

- R3.** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-~~76~~ 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-~~76~~ Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

CIP-004- 76 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-76 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 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. <p>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.</p>	<p>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.</p>

CIP-004-~~76~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~76~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none">1. EACMS; and2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none">1. EACMS; and2. PACS	<p>Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.</p>

CIP-004-~~76~~ — Cyber Security – Personnel & Training

- 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-~~76~~ 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-~~76~~ 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- 76 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; <u>and</u> 4.1.2. Unescorted physical access into a Physical Security Perimeter; <u>and</u> 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access <u>and</u> unescorted physical access in a Physical Security Perimeter, <u>and</u> access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~76~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~76~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 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.

CIP-004- 6 Table R4—Assess-Management-Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> — EACMS; and 1. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ul style="list-style-type: none"> 0. EACMS; and 0. PACS 	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ul style="list-style-type: none"> 0. A dated listing of authorizations for BES Cyber System information; 0. Any privileges associated with the authorizations; and 0. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

- 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-~~76~~ 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-~~76~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004- 76 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004- 76 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~76~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.3	<p>High Impact BES Cyber Systems and their associated: EACMS; and PACS</p> <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: EACMS; and PACS</p>	<p>For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.</p>
5. 3 4	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.</p>	<p>An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.</p>

CIP-004-~~76~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5. 45	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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.</p> <p>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.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> Workflow or sign-off form showing password reset within 30 calendar days of the termination; Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

- 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-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 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-004-7 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-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.1	<u>High Impact BES Cyber Systems and their associated:</u> <ol style="list-style-type: none"> <u>EACMS; and</u> <u>PACS</u> <u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u> <ol style="list-style-type: none"> <u>EACMS; and</u> <u>PACS</u> 	<u>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:</u> <ol style="list-style-type: none"> <u>6.1.1. Provisioned electronic access to electronic BCSI; and</u> <u>6.1.2. Provisioned physical access to physical BCSI.</u> 	<u>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.</u>

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	Applicable Systems	Requirements	Measures
6.2	<p><u>High Impact BES Cyber Systems and their associated:</u></p> <ol style="list-style-type: none"> <u>1. EACMS; and</u> <u>2. PACS</u> <p><u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u></p> <ol style="list-style-type: none"> <u>1. EACMS; and</u> <u>2. PACS</u> 	<p><u>Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:</u></p> <ol style="list-style-type: none"> <u>6.2.1. have an authorization record; and</u> <u>6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.</u> 	<p><u>Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following:</u></p> <ul style="list-style-type: none"> <u>• List of authorized individuals;</u> <u>• List of individuals who have been provisioned access;</u> <u>• Verification that provisioned access is appropriate based on need; and</u> <u>• Documented reconciliation actions, if any.</u>
6.3	<p><u>High Impact BES Cyber Systems and their associated:</u></p> <ol style="list-style-type: none"> <u>1. EACMS; and</u> <u>2. PACS</u> <p><u>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</u></p> <ol style="list-style-type: none"> <u>1. EACMS; and</u> <u>2. PACS</u> 	<p><u>For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.</u></p>	<p><u>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.</u></p>

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

- ~~Each Responsible~~ The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- ~~If a Responsible~~ 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 ~~Enforce~~ Assessment ~~Program~~ 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.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot-Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

1.4. ~~Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>	<p>The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15</p>	<p>The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</p>	<p>security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)</p> <p>OR</p> <p>The Responsible Entity implemented a cyber security training program but failed to</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	Operations Planning	Medium	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct</p>	<p>The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,</p>	<p>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 (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3)</p> <p>OR</p> <p>The Responsible Entity has a program for</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service</p>	<p>Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in</p>	<p>including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4)</p> <p>OR</p>	<p>conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4)</p> <p>OR</p> <p>The Responsible Entity has a process to perform</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</p>	<p>3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments</p>	<p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</p>	<p>seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)</p> <p>OR</p> <p>The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	Operations Planning and Same Day Operations	Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) 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. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has did not implemented one or more documented program(s) for access management that includes a process to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information</p>	<p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented</p>	<p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is</p>	<p>authorize electronic access, or unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)</p> <p>OR</p> <p>The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2)</p> <p>OR</p> <p>The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			storage locations, privileges were incorrect or unnecessary. (4.4)	processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Same Day Operations and Operations Planning	Medium	<p>The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.43)</p> <p>OR</p> <p>The Responsible Entity has implemented one or</p>	<p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following</p>	<p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized</p>	<p>The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, <u>or</u> unescorted physical access, or BES Cyber System Information storage locations. (R5)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)</p> <p>OR</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<p>more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.45)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the</p>	<p>reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)</p>	<p>electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)</p>	<p>The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)</p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004- 76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances. (5. 54)	day following the effective date and time of the termination action. (5.3)		
R6	<u>Same Day Operations and Operations Planning</u>	<u>Medium</u>	<p><u>The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)</u></p>	<p><u>The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months</u></p>	<p><u>The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the</u></p>	<p><u>The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1)</u></p> <p><u>OR</u></p>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			<u>OR</u> <u>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.</u>	<u>but less than or equal to 17 calendar months of the previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.</u>	<u>previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.</u>	<u>The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2)</u> <u>OR</u> <u>The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.</u>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
<u>7</u>	<u>8/12/21</u>	<u>Adopted by the NERC Board of Trustees</u>	<u>Revised to enhance BES reliability for entities to manage their BCSl.</u>

Guidelines and Technical Basis

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

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

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

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

~~Requirement R1:~~

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

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

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

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

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

~~Requirement R2:~~

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

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

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

Requirement R3:

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

~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven year check could not be performed. Examples of this~~

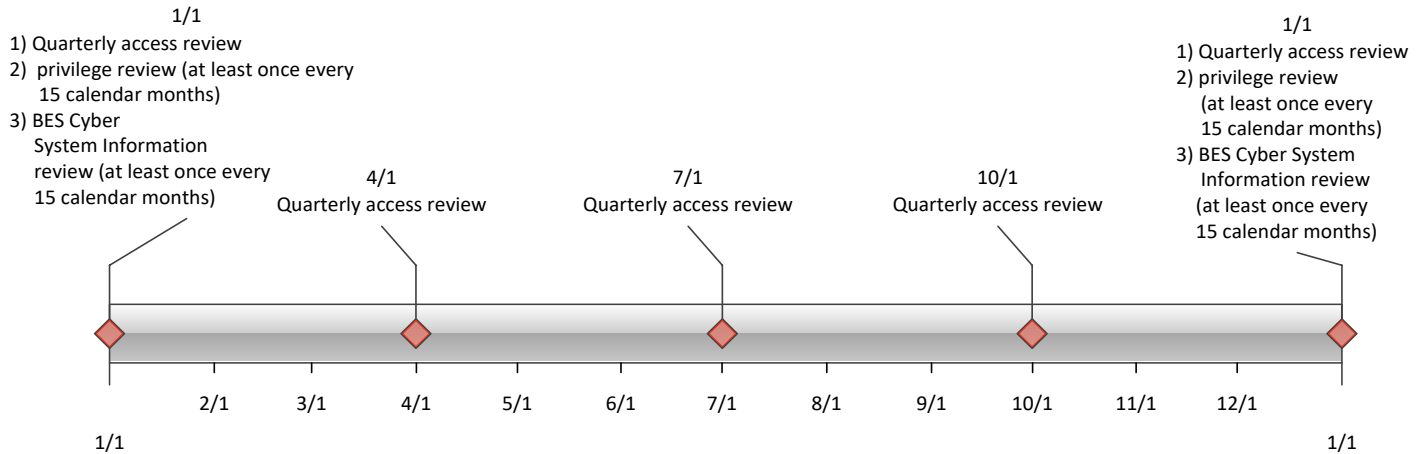
~~could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining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

Requirement R4:

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

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

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



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

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

Rationale:

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

Rationale for Requirement R1:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

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

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

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

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

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

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

Rationale for Requirement R5:

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

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

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

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

Exhibit A-3

CIP-011-3
Clean

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-3
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
 - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
 - 4.1.1 **Balancing Authority**
 - 4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
 - 4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
 - 4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
 - 4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
 - 4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
 - 4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
 - 4.1.3 **Generator Operator**
 - 4.1.4 **Generator Owner**
 - 4.1.5 **Reliability Coordinator**

4.1.6 Transmission Operator**4.1.7 Transmission Owner**

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-011-3.

6. Background: Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and

implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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

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

“Applicable Systems” Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 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-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Method(s) to identify BCSI.	<p>Examples of acceptable evidence may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • 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.

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	<p>Examples of evidence for on-premise BCSI may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). <p>Examples of evidence for off-premise BCSI may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • 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

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
			<ul style="list-style-type: none">• 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-011-3 Table R2 – BES Cyber Asset 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-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.</p>	<p>Examples of acceptable evidence may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • 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 or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.</p>	<p>Examples of acceptable evidence may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	<p>The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1)</p> <p>OR</p> <p>The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1)</p> <p>OR</p> <p>The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)</p>	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	Operations Planning	Lower	N/A	The Responsible Entity implemented one or more documented processes but did	The Responsible Entity implemented one or more documented processes but did	The Responsible Entity has not documented or implemented any processes for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSl.

Exhibit A-3

CIP-011-3
Redline

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-~~32~~
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

~~4.1.5 Interchange Coordinator or Interchange Authority~~

~~4.1.6~~ 4.1.5 Reliability Coordinator

4.1.74.1.6 Transmission Operator**4.1.84.1.7 Transmission Owner**

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~32~~:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-011-~~32~~.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

“Applicable Systems” Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in CIP-011-3 Table R1 – Information Protection Program that collectively includes each of the applicable requirement parts in CIP-011-~~32~~ 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-~~32~~ Table R1 – Information Protection Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-23 Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Method(s) to identify information that meets the definition of BES Cyber system Information <u>BCSI</u> .	<p>Examples of acceptable evidence <u>may</u> include, but are not limited to, <u>the following</u>:</p> <ul style="list-style-type: none"> • Documented method(s) to identify BES Cyber System Information <u>BCSI</u> from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information <u>BCSI</u> as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BES Cyber System Information <u>BCSI</u>; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program. • <u>Storage locations identified for housing BCSI in the entity's information protection program.</u>

CIP-011-23 Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Procedure(s) for protecting and Method(s) to protect and securely handling BES Cyber System Information BCSI, including storage, transit, and use to mitigate risks of compromising confidentiality.</p>	<p>Examples of acceptable evidence <u>for on-premise BCSI may include</u>, but are not limited to, <u>the following</u>:</p> <ul style="list-style-type: none"> • Procedures for protecting and securely handling <u>BCSI</u>, which include topics such as storage, security during transit, and use of BES Cyber System information; or • Records indicating that BES Cyber System Information BCSI is handled in a manner consistent with the entity's documented procedure(s). <p><u>Examples of evidence for off-premise BCSI may include, but are not limited to, the following</u>:</p> <ul style="list-style-type: none"> • <u>Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or</u> • <u>Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical</u>

CIP-011-~~33~~ Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
			<u>badge management, biometrics, alarm system); or</u> <ul style="list-style-type: none">• <u>Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).</u>

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-~~32~~ Table R2 – BES Cyber Asset 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-~~32~~ Table R2 – BES Cyber Asset Reuse and Disposal and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011- 32 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information <u>BCSI</u> (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information <u>BCSI</u> from the Cyber Asset data storage media.</p>	<p>Examples of acceptable evidence <u>may</u> include, but are not limited to, <u>the following</u>:</p> <ul style="list-style-type: none"> • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information <u>BCSI</u> such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information <u>BCSI</u>.

CIP-011-~~32~~ Table R2 – BES Cyber Asset Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	<p>Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information<u>BCSI</u>, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information<u>BCSI</u> from the Cyber Asset or destroy the data storage media.</p>	<p>Examples of acceptable evidence <u>may</u> include, but are not limited to, <u>the following</u>:</p> <ul style="list-style-type: none"> • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information<u>BCSI</u> prior to the disposal of an applicable Cyber Asset.

B. 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, 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 the NERC Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA 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 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~~ The applicable E entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~Responsible applicable E~~ entity is found non-compliant, it shall keep information related to the noncompliance 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 Process~~ Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~3 Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- 23)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	<p><u>The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1)</u></p> <p><u>OR</u></p> <p><u>The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)</u></p> <p>N/A</p>	<p>The Responsible Entity has not <u>neither</u> documented nor implemented a <u>one or more BES Cyber System Information</u> BCSI protection program(s). (R1)</p>
R2	Operations Planning	Lower	N/A	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity implemented one or more documented processes but did not include disposal or	The Responsible Entity has not documented or implemented any processes for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011- 23)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information <u>BCSI</u> from the BES Cyber Asset. (2.1)	media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information <u>BCSI</u> from the BES Cyber Asset. (2.2)	applicable requirement parts in CIP-011- 32 Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents**Version History**

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	

<u>3</u>	<u>TBD</u>	<u>Adopted by the NERC Board of Trustees</u>	<u>Revised to enhance BES reliability for entities to manage their BCSl.</u>
----------	------------	--	--

Guidelines and Technical Basis

Section 4 — Scope of Applicability of the CIP Cyber Security Standards

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

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

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

Requirement R1:

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need to know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

Requirement R2:

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the~~

~~analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~

~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.~~

~~Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.~~

Rationale:

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

Rationale for Requirement R1:

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

Rationale for Requirement R2:

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

Exhibit B

List of Currently Effective NERC Reliability Standards

Standard Version	Title
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-3	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-003-8	Cyber Security — Security Management Controls
CIP-004-6	Cyber Security — Personnel & Training
CIP-005-6	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-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security — Information Protection
CIP-013-1	Cyber Security - Supply Chain Risk Management
CIP-014-2	Physical Security
COM-001-3	Communications
COM-002-4	Operating Personnel Communications Protocols
EOP-004-4	Event Reporting

Standard Version	Title
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-011-1	Emergency Operations
FAC-001-3	Facility Interconnection Requirements
FAC-002-3	Facility Interconnection Studies
FAC-003-4	Transmission Vegetation Management
FAC-008-5	Facility Ratings
FAC-010-3	System Operating Limits Methodology for the Planning Horizon
FAC-011-3	System Operating Limits Methodology for the Operations Horizon
FAC-014-2	Establish and Communicate System Operating Limits
FAC-501-WECC-2	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-008-2	Reliability Coordinator Operational Analyses and Real-time Assessments
IRO-009-2	Reliability Coordinator Actions to Operate Within IROLs
IRO-010-3	Reliability Coordinator Data Specification and Collection
IRO-014-3	Coordination Among Reliability Coordinators

Standard Version	Title
IRO-017-1	Outage Coordination
IRO-018-1(i)	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities
MOD-001-1a	Available Transmission System Capability
MOD-004-1	Capacity Benefit Margin
MOD-008-1	Transmission Reliability Margin Calculation Methodology
MOD-025-2	Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability
MOD-026-1	Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions
MOD-027-1	Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions
MOD-028-2	Area Interchange Methodology
MOD-029-2a	Rated System Path Methodology
MOD-030-3	Flowgate Methodology
MOD-031-3	Demand and Energy Data
MOD-032-1	Data for Power System Modeling and Analysis
MOD-033-2	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-002-2	Disturbance Monitoring and Reporting Requirements
PRC-004-6	Protection System Misoperation Identification and Correction
PRC-005-1.1b	Transmission and Generation Protection System Maintenance and Testing
PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

Standard Version	Title
PRC-006-5	Automatic Underfrequency Load Shedding
PRC-006-NPCC-2	Automatic Underfrequency Load Shedding
PRC-006-SERC-02	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-018-1	Disturbance Monitoring Equipment Installation and Data Reporting
PRC-019-2	Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection
PRC-023-4	Transmission Relay Loadability
PRC-024-2	Generator Frequency and Voltage Protective Relay Settings
PRC-025-2	Generator Relay Loadability
PRC-026-1	Relay Performance During Stable Power Swings
PRC-027-1	Coordination of Protection Systems for Performance During Faults
TOP-001-5	Transmission Operations
TOP-002-4	Operations Planning
TOP-003-4	Operational Reliability Data
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities
TPL-001-4	Transmission System Planning Performance Requirements
TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events
VAR-001-5	Voltage and Reactive Control

Standard Version	Title
VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules
VAR-501-WECC-3.1	Power System Stabilizer (PSS)

Exhibit C

Updated Glossary of Terms Used in NERC Reliability Standards

Glossary of Terms Used in NERC Reliability Standards

Updated June 28, 2021

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 June 28, 2021.

This reference is divided into four sections, and each section is organized in alphabetical order.

Subject to Enforcement

Pending Enforcement

Retired Terms

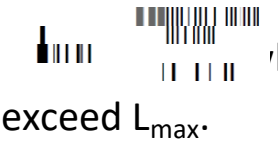
Regional Definitions

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 following NERC's Reliability Standards Development Process, and added to this glossary following board adoption, with the "FERC effective" date added following a final Order approving the definition.

Any comments regarding this glossary should be reported to the NERC Help Desk at <https://support.nerc.net/>. Select "Standards" from the Applications drop down menu and "Other" from the Standards Subcategories drop down menu.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Actual Frequency (F _A)	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	The Interconnection frequency measured in Hertz (Hz).
Actual Net Interchange (NI _A)	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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		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		A time classification assigned to an RFI when the submittal time is greater than one hour after the start time of the RFI.
Agreement	Version 0 Reliability Standards		2/8/2005	3/16/2007		A contract or arrangement, either written or verbal and sometimes enforceable by law.
Alternative Interpersonal Communication	Project 2006-06		11/7/2012	4/16/2015	10/1/2015	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		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 <u>minimum vegetation clearance distances</u> .
Ancillary Service	Version 0 Reliability Standards		2/8/2005	3/16/2007		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. <i>(From FERC order 888-A.)</i>
Anti-Aliasing Filter	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards	ACE	12/19/2012	10/16/2013	4/1/2014	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 <u>Balancing Authorities in the Western Interconnection</u> .
Area Interchange Methodology	Project 2006-07		8/22/2008	11/24/2009		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 <u>generally reported on an area to area basis</u> .
Arranged Interchange	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	The state where a Request for Interchange (initial or revised) has been submitted for approval.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Attaining Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	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 2010-14.2.1. Phase 2	AGC	2/11/2016	9/20/2017	1/1/2019	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.
Automatic Time Error Correction (I_{ATEC})	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	<ul style="list-style-type: none"> • $Y = B_i / B_S$. • 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 $(1-Y) * (II_{actual} - B_i * \Delta TE/6)$ • 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: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t) * (TE_{offset})$
Automatic Time Error Correction (I_{ATEC})	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	<ul style="list-style-type: none"> • 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 PIIhourly in MWh. An On-Peak and Off-Peak accumulation accounting is required, where: $PII_{accum}^{on/offpeak} = last\ period's\ PII_{accum}^{on/offpeak} + PII_{hourly}$
Automatic Time Error Correction (I_{ATEC}) <i>continued below...</i>	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	<p>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.</p>  <p>When operating in Automatic Time error correction Mode. The absolute value of I_{ATEC} shall not exceed L_{max}.</p> <p>I_{ATEC} Shall be zero when operating in any other AGC mode.</p> <ul style="list-style-type: none"> • L_{max} is the maximum value allowed for I_{ATEC} set by each BA between $0.2 * B_i$ and L_{10}, $0.2 * B_i \leq L_{max} \leq L_{10}$. • $L_{10} = 1.65$ • ϵ_{10} is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-r... $\epsilon_{10} = \sqrt{\frac{(-10B_i)(-10B_S)}{...}}$ 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Available Flowgate Capability	Project 2006-07	AFC	8/22/2008	11/24/2009		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		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		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	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.
Balancing Authority Area	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	<p>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.</p> <p>A. Sudden loss of generation:</p> <ul style="list-style-type: none"> a. Due to <ul style="list-style-type: none"> 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; b. And, that causes an unexpected change to the responsible entity's ACE; <p>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.</p> <p>C. Sudden restoration of a Demand that was used as a resource that causes an unexpected change to the responsible entity's ACE.</p>
Base Load	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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 equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
BES Cyber System	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	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	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	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.
Block Dispatch	Project 2006-07		8/22/2008	11/24/2009		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 (continued below)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (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: <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Bulk Electric System (continued below)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Implementation Plan for Phase 2 Compliance obligations.)	<ul style="list-style-type: none"> • 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 facilities designated as BES are: <ul style="list-style-type: none"> 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.
Bulk Electric System (continued)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Implementation Plan for Phase 2 Compliance obligations.)	<p>Exclusions:</p> <ul style="list-style-type: none"> • E1 - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: <ul style="list-style-type: none"> 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). <p>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.</p> <p>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.</p>
Bulk Electric System (continued)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Implementation Plan for Phase 2 Compliance obligations.)	<ul style="list-style-type: none"> • 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Bulk Electric System (continued)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Implementation Plan for Phase 2 Compliance obligations.)	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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
Bulk Electric System (continued)	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Implementation Plan for Phase 2 Compliance obligations.)	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 Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL). <ul style="list-style-type: none"> • 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	Bulk-Power System: (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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	A circuit breaker that is positioned to connect two individual substation bus configurations.
Capacity Benefit Margin	Version 0 Reliability Standards	CBM	2/8/2005	3/16/2007		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 generation reliability requirements. The transmission transfer

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Capacity Benefit Margin Implementation Document	Project 2006-07	CBMID	11/13/2008	11/24/2009		A document that describes the implementation of a Capacity Benefit Margin methodology.
Capacity Emergency	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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	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	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.
Clock Hour	Version 0 Reliability Standards		2/8/2005	3/16/2007		The 60-minute period ending at :00. All surveys, measurements, and reports are based on Clock Hour periods unless specifically noted.
Cogeneration	Version 0 Reliability Standards		2/8/2005	3/16/2007		Production of electricity from steam, heat, or other forms of energy produced as a by-product of another process.
Compliance Monitor	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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	2010-05.1		8/14/2014	5/13/2015	7/1/2016	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	The state where no party has denied and all required parties have approved the Arranged Interchange.
Congestion Management Report	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		A transmission facility (line, transformer, breaker, etc.) that is approaching, is at, or is beyond its System Operating Limit or Interconnection Reliability Operating Limit.
Contact Path	Version 0 Reliability Standards		2/8/2005	3/16/2007		An agreed upon electrical path for the continuous flow of electrical power between the parties of an Interchange Transaction.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Contingency	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 Phase 1		11/5/2015	1/19/2017	1/1/2018	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 Phase 1		11/5/2015	1/19/2017	1/1/2018	<p>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:</p> <ul style="list-style-type: none"> • 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 Phase 1		11/5/2015	1/19/2017	1/1/2018	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	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.
Control Performance Standard	Version 0 Reliability Standards	CPS	2/8/2005	3/16/2007		The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period.
Corrective Action Plan	Phase III-IV Planning Standards - Archive		2/7/2006	3/16/2007		A list of actions and an associated timetable for implementation to remedy a specific problem.
Cranking Path	Phase III-IV Planning Standards - Archive		5/2/2006	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.
Curtailment Threshold	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Programmable electronic devices, including the hardware, software, and data in those devices.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Cyber Security Incident	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		2/7/2019	6/20/2019	1/1/2021	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.
Delayed Fault Clearing	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/1/2006	12/27/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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	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		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		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.
Distribution Factor	Version 0 Reliability Standards	DF	2/8/2005	3/16/2007		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	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Disturbance Control Standard	Version 0 Reliability Standards	DCS	2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Disturbance Monitoring Equipment	Phase III-IV Planning Standards	DME	8/2/2006	3/16/2007		Devices capable of monitoring and recording system data pertaining to a Disturbance. Such devices include the following categories of recorders* : <ul style="list-style-type: none"> • 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 excursions *Phasor Measurement Units and any other equipment that meets the functional requirements of DMEs may qualify as DMEs.
Dynamic Interchange Schedule or Dynamic Schedule	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	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).
Dynamic Transfer	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		The allocation of demand to individual generating units on line to effect the most economical production of electricity.
Electrical Energy	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 Order 706	EACMS	11/26/2012	11/22/2013	7/1/2016	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 Order 706	EAP	11/26/2012	11/22/2013	7/1/2016	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 Order 706	ESP	11/26/2012	11/22/2013	7/1/2016	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	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An Element may be comprised of one or more components.
Emergency or BES Emergency	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 Coordinate Interchange	Emergency RFI	10/29/2008	12/17/2009		Request for Interchange to be initiated for Emergency or Energy Emergency conditions.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Energy Emergency	Version 0		11/13/2014	11/19/2015	4/1/2017	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		2/7/2006	3/16/2007		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		Committed uses of a Transmission Service Provider's Transmission system considered when determining ATC or AFC.
External Routable Connectivity	Project 2008-06 Order 706		11/26/2012	11/22/2013	7/1/2016	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.
Facility	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		2/7/2006	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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		The likelihood that a fire will ignite or spread in a particular geographic area.
Firm Demand	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		The highest quality (priority) service offered to customers under a filed rate schedule that anticipates no planned interruption.
Flashover	Project 2007-07		2/7/2006	3/16/2007		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		8/22/2008	11/24/2009		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	Version 0 Reliability Standards		8/22/2008	11/24/2009		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).

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Forced Outage	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Frequency Bias	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 2007-12		2/7/2013	1/16/2014	4/1/2015	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.
Frequency Deviation	Version 0 Reliability Standards		2/8/2005	3/16/2007		A change in Interconnection frequency.
Frequency Error	Version 0 Reliability Standards		2/8/2005	3/16/2007		The difference between the actual and scheduled frequency. ($F_A - F_S$)
Frequency Regulation	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		(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	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	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.
Frequency Response Sharing Group	Project 2007-12	FRSG	2/7/2013	1/16/2014	4/1/2015	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 ATC/TTC/AFC and CBM/TRM Revisions	GCIR	11/13/2008	11/24/2009		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 Operator	Version 0 Reliability Standards	GOP	11/5/2015	1/21/2016	7/1/2016	The entity that operates generating Facility(ies) and performs the functions of supplying energy and Interconnected Operations Services.
Generator Owner	Version 0 Reliability Standards	GO	11/5/2015	1/21/2016	7/1/2016	Entity that owns and maintains generating Facility(ies).
Generator Shift Factor	Version 0 Reliability Standards	GSF	2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Generator-to-Load Distribution Factor	Version 0 Reliability Standards	GLDF	2/8/2005	3/16/2007		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 Assessment	Project 2013-03 Geomagnetic Disturbance Mitigation	GMD	12/17/2014	9/22/2016	7/1/2017	Documented evaluation of potential susceptibility to voltage collapse, Cascading, or localized damage of equipment due to geomagnetic disturbances.
Host Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		Data measured on a Clock Hour basis.
Implemented Interchange	Coordinate Interchange		5/2/2006	3/16/2007		The state where the Balancing Authority enters the Confirmed Interchange into its Area Control Error equation.
Inadvertent Interchange	Version 0 Reliability Standards		2/8/2005	3/16/2007		The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. (IA – IS)
Independent Power Producer	Version 0 Reliability Standards	IPP	2/8/2005	3/16/2007		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		
Interactive Remote Access	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	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 communications.
Interchange	Coordinate Interchange		5/2/2006	3/16/2007		Energy transfers that cross Balancing Authority boundaries.
Interchange Authority	Project 2015-04	IA	11/5/2015	1/21/2016	7/1/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Interchange Meter Error (I _{ME})	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	A term used in the Reporting ACE calculation to compensate for data or equipment errors affecting any other components of the Reporting ACE calculation.
Interchange Schedule	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Interchange Transaction	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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	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		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 T _v	Determine Facility Ratings, Operating Limits, and Transfer Capabilities	IROL T _v	11/1/2006	12/27/2007		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 T _v shall be less than or equal to 30 minutes.
Intermediate Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	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	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 located inside the Electronic Security Perimeter.
Interpersonal Communication	Project 2006-06		11/7/2012	4/16/2015	10/1/2015	Any medium that allows two or more individuals to interact, consult, or exchange information.
Interruptible Load or Interruptible Demand	Version 0 Reliability Standards		11/1/2006	3/16/2007		Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment.
Joint Control	Version 0 Reliability Standards		2/8/2005	3/16/2007		Automatic Generation Control of jointly owned units by two or more Balancing Authorities.
Limiting Element	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Load	Version 0 Reliability Standards		2/8/2005	3/16/2007		An end-use device or customer that receives power from the electric system.
Load Shift Factor	Version 0 Reliability Standards	LSF	2/8/2005	3/16/2007		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	Secures energy and Transmission Service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.
Long-Term Transmission Planning Horizon	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	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 Reliability Coordination - Transmission Loading Relief		11/4/2010	4/21/2011		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	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	<p>The failure of a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:</p> <p>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.</p> <p>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.</p> <p>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. (continued below...)</p>

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Misoperation (continued...)	Project 2010-05.1		8/14/2014	5/13/2015	7/1/2016	<p>4. Slow Trip – Other Than Fault – A Composite Protection 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.</p> <p>5. Unnecessary Trip – During Fault – An unnecessary Composite Protection System operation for a Fault condition on another Element.</p> <p>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.</p>
Most Severe Single Contingency	Project 2010-14.1 Phase 1	MSSC	11/5/2015	1/19/2017	1/1/2018	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).
Native Balancing Authority	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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		The transmission planning period that covers Year One through five.
Net Actual Interchange	Version 0 Reliability Standards		2/8/2005	3/16/2007		The algebraic sum of all metered interchange over all interconnections between two physically Adjacent Balancing Authority Areas.
Net Energy for Load	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Net Interchange Schedule	Version 0 Reliability Standards		2/8/2005	3/16/2007		The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.
Net Scheduled Interchange	Version 0 Reliability Standards		2/8/2005	3/16/2007		The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time.
Network Integration Transmission Service	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Non-Consequential Load Loss	Project 2006-02		8/4/2011	10/17/2013	1/1/2015	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		Transmission service that is reserved on an as-available basis and is subject to curtailment or interruption.
Non-Spinning Reserve	Version 0 Reliability Standards		2/8/2005	3/16/2007		1. That generating reserve not connected to the system but capable of serving demand within a specified time. 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		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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		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		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		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		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of lower electrical demand.
On-Peak	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards	OASIS	2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Open Access Transmission Tariff	Version 0 Reliability Standards	OATT	2/8/2005	3/16/2007		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	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		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.
Operational Planning Analysis	Project 2007-06.2 Phase 2 of System Protection Coordination	OPA	8/11/2016	6/7/2018	4/1/2021	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.)
Operating Procedure	Coordinate Operations		2/7/2006	3/16/2007		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 specific transmission line from service is an example of an Operating Procedure.
Operating Process	Coordinate Operations		2/7/2006	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		The portion of Operating Reserve consisting of: <ul style="list-style-type: none"> • 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Operating Reserve – Supplemental	Version 0 Reliability Standards		2/8/2005	3/16/2007		The portion of Operating Reserve consisting of: <ul style="list-style-type: none"> • 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		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 value.
Operational Planning Analysis	Project 2014-03	OPA	11/13/2014	11/19/2015	1/1/2017	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 Special Protection System status or degradation; 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	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 ATC/TTC/AFC and CBM/TRM Revisions	OTDF	8/22/2008	11/24/2009		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		A method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing Authority's actual interchange, frequency response, and schedules into providing Balancing Authority's AGC/ACE equation.
Participation Factors	Project 2006-07 ATC/TTC/AFC and CBM/TRM Revisions		8/22/2008	11/24/2009		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.
Peak Demand	Version 0 Reliability Standards		2/8/2005	3/16/2007		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		2/7/2006	3/16/2007		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 Cyber Security Order 706	PACS	11/26/2012	11/22/2013	7/1/2016	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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Physical Security Perimeter	Project 2008-06 Cyber Security Order 706	PSP	11/26/2012	11/22/2013	7/1/2016	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 Assess Transmission Future Needs and Develop Transmission Plans		8/4/2011	10/17/2013	1/1/2015	Documented evaluation of future Transmission System performance and Corrective Action Plans to remedy identified deficiencies.
Planning Authority	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	The responsible entity that coordinates and integrates transmission Facilities and service plans, resource plans, and Protection Systems.
Planning Coordinator	Project 2006-07 ATC/TTC/AFC and CBM/TRM Revisions	PC	8/22/2008	11/24/2009		See Planning Authority.
Point of Delivery	Version 0 Reliability Standards	POD	2/8/2005	3/16/2007		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.
Point of Receipt	Project 2015-04 Alignment of Terms	POR	11/5/2015	1/21/2016	7/1/2016	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	Version 0 Reliability Standards	PTP	2/8/2005	3/16/2007		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 ATC/TTC/AFC and CBM/TRM Revisions	PTDF	8/22/2008	11/24/2009		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 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Protection System	Project 2007-17 Protection System Maintenance and Testing		11/19/2010	2/3/2012	4/1/2013	Protection System – <ul style="list-style-type: none"> • 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 • 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 System Protection Coordination		11/5/2015	6/7/2018	4/1/2021	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 PRC-005 FERC Order No 803 Directive	PSMP	11/5/2015	12/18/2015	1/1/2016	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: <ul style="list-style-type: none"> • 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 2010-14.2.1. Phase 2		2/11/2016	9/20/2017	1/1/2019	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).
Purchasing-Selling Entity	Version 0 Reliability Standards	PSE	2/8/2005	3/16/2007		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.
Ramp Rate or Ramp	Version 0 Reliability Standards		2/8/2005	3/16/2007		(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 Transmission Vegetation Management		2/7/2006	3/16/2007		The specified or reasonably anticipated conditions under which the electrical system or an individual electrical circuit is intend/designed to operate

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Rated System Path Methodology	Project 2006-07 ATC/TTC/AFC and CBM/TRM Revisions		8/22/2008	11/24/2009		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		The operational limits of a transmission system element under a set of specified conditions.
Reactive Power	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	The portion of electricity that supplies energy to the Load.
Real-time	Coordinate Operations		2/7/2006	3/16/2007		Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)
Real-time Assessment	Project 2007-06.2 Phase 2 of System Protection Coordination	RTA	8/11/2016	6/8/2018	4/1/2021	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		The Balancing Authority importing the Interchange.
Regional Reliability Organization	Version 0 Reliability Standards	RRO	2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Regulation Reserve Sharing Group	Project 2010-14.1 Phase 1		8/15/2013	4/16/2015	7/1/2016	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.
Regulation Service	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 as specified by NERC for itself and the Balancing Authority for which it is providing the Regulation Service.
Reliability Adjustment Arranged Interchange	Project 2008-12 Coordinate Interchange Standards		2/6/2014	6/30/2014	10/1/2014	A request to modify a Confirmed Interchange or Implemented Interchange for reliability purposes.
Reliability Adjustment RFI	Project 2007-14 Coordinate Interchange - Timing Table		10/29/2008	12/17/2009		Request to modify an Implemented Interchange Schedule for reliability purposes.
Reliability Coordinator	Project 2015-04 Alignment of Terms	RC	11/5/2015	1/21/2016	7/1/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards	RCIS	2/8/2005	3/16/2007		The system that Reliability Coordinators use to post messages and share operating information in real time.
Reliability Standard	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Remedial Action Scheme	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>The following do not individually constitute a RAS:</p> <ol style="list-style-type: none"> a. Protection Systems installed for the purpose of detecting Faults on BES Elements and isolating the faulted Elements 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
Remedial Action Scheme <i>Continued</i>	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	<ol style="list-style-type: none"> 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 m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities (e.g., currents or torsional oscillations)
Remedial Action Scheme <i>Continued</i>	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	<ol style="list-style-type: none"> 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

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Removable Media	Project 2016-02 Modifications to CIP Standards		2/9/2017	4/19/2018	1/1/2020	<p>Storage media that:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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. <p>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</p>
Reportable Balancing Contingency Event	Project 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	<p>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 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.</p> <ul style="list-style-type: none"> • Eastern Interconnection – 900 MW • Western Interconnection – 500 MW • ERCOT – 800 MW • Quebec – 500 MW
Reportable Cyber Security Incident	Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		2/7/2019	6/20/2019	1/1/2021	<p>A Cyber Security Incident that compromised or disrupted:</p> <ul style="list-style-type: none"> - 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.
Reportable Disturbance	Version 0 Reliability Standards		2/8/2005	3/16/2007		<p>Any event that causes an 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.</p>

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Reporting ACE	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	<p>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).</p> <p>Reporting ACE is calculated as follows: $\text{Reporting ACE} = (NI_A - NI_S) - 10B (F_A - FS) - I_{ME}$</p> <p>Reporting ACE is calculated in the Western Interconnection as follows: $\text{Reporting ACE} = (NI_A - NI_S) - 10B (F_A - FS) - I_{ME} + I_{ATEC}$</p> <p>Where:</p> <ul style="list-style-type: none"> • 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_{ATEC} = Automatic Time Error Correction.
Reporting ACE (continued)	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	<p>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 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:</p> <ol style="list-style-type: none"> 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 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 F_S 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 Coordinate Interchange	RFI	2/6/2014	6/30/2014	10/1/2014	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 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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 quicker (e.g., between zero and ten minutes) then, for the purposes of disturbance control performance, the areas become a Reserve Sharing Group.
Reserve Sharing Group Reporting ACE	Project 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	At any given time of measurement for the applicable Reserve Sharing Group (RSG), the algebraic sum of the ACEs (or equivalent as calculated at such time of measurement) of the Balancing Authorities participating in the RSG at the time of measurement.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Resource Planner	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	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 forementioned criteria
Scenario	Coordinate Operations		2/7/2006	3/16/2007		Possible event.
Schedule	Version 0 Reliability Standards		2/8/2005	3/16/2007		(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.
Scheduled Frequency	Version 0 Reliability Standards		2/8/2005	3/16/2007		60.0 Hertz, except during a time correction.
Scheduled Net Interchange (NI _s)	Project 2010-14.2.1 Phase 2		2/11/2016		7/1/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		An entity responsible for approving and implementing Interchange Schedules.
Scheduling Path	Version 0 Reliability Standards		2/8/2005	3/16/2007		The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.
Sending Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007		The Balancing Authority exporting the Interchange.
Sink Balancing Authority	Project 2008-12 Coordinate Interchange Standards		2/6/2014	6/30/2014	10/1/2014	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 Coordinate Interchange Standards		2/6/2014	6/30/2014	10/1/2014	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	See "Remedial Action Scheme"

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Spinning Reserve	Version 0 Reliability Standards		2/8/2005	3/16/2007		Unloaded generation that is synchronized and ready to serve additional demand.
Stability	Version 0 Reliability Standards		2/8/2005	3/16/2007		The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances.
Stability Limit	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards	SCADA	2/8/2005	3/16/2007		A system of remote control and telemetry used to monitor and control the transmission system.
Supplemental Regulation Service	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 ACE.
Surge	Version 0 Reliability Standards		2/8/2005	3/16/2007		A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.
Sustained Outage	Project 2007-07 Transmission Vegetation Management		2/7/2006	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		A combination of generation, transmission, and distribution components.
System Operating Limit	Project 2015-04 Alignment of Terms	SOL	11/5/2015	1/21/2016	7/1/2016	<p>The value (such as MW, Mvar, amperes, frequency or volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to:</p> <ul style="list-style-type: none"> • Facility Ratings (applicable pre- and post-Contingency Equipment Ratings or Facility Ratings) • transient stability ratings (applicable pre- and post- Contingency stability limits) • voltage stability ratings (applicable pre- and post-Contingency voltage stability) • system voltage limits (applicable pre- and post-Contingency voltage limits)
System Operator	Project 2010-01 Training		2/6/2014	6/19/2014	7/1/2016	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.
Telemetry	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Tie Line	Version 0 Reliability Standards		2/8/2005	3/16/2007		A circuit connecting two Balancing Authority Areas.
Tie Line Bias	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 caused by the accumulation of Frequency Error over a given period.
Time Error Correction	Version 0 Reliability Standards		2/8/2005	3/16/2007		An offset to the Interconnection's scheduled frequency to return the Interconnection's Time Error to a predetermined value.
TLR (Transmission Loading Relief) Log (NERC added the spelled out term for TLR Log for clarification purposes.)	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Total Flowgate Capability	Project 2006-07 ATC/TTC/AFC and CBM/TRM Revisions	TFC	8/22/2008	11/24/2009		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 Demand Data (MOD C)		5/6/2014	2/19/2015	7/1/2016	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	Version 0 Reliability Standards	TTC	2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		See Interchange Transaction.
Transfer Capability	Version 0 Reliability Standards		2/8/2005	3/16/2007		The measure of the ability of interconnected electric systems to move or transfer power <i>in a reliable manner</i> 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 <i>not</i> generally equal to the transfer capability from "Area B" to "Area A."
Transfer Distribution Factor	Version 0 Reliability Standards		2/8/2005	3/16/2007		See Distribution Factor.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Transient Cyber Asset	Project 2016-02 Modifications to CIP Standards	TCA	2/9/2017	4/19/2018	1/1/2020	<p>A Cyber Asset that is:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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. <p>Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.</p>
Transmission	Version 0 Reliability Standards		2/8/2005	3/16/2007		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		A limitation on one or more transmission elements that may be reached during normal or contingency system operations.
Transmission Customer	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	<ol style="list-style-type: none"> 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.
Transmission Line	Project 2007-07 Transmission Vegetation Management		2/7/2006	3/16/2007		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 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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 ATC/TTC/AFC and CBM/TRM Revisions		8/22/2008	11/24/2009		The collection of Transmission assets over which the Transmission Operator is responsible for operating.
Transmission Owner	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	The entity that owns and maintains transmission Facilities.
Transmission Planner	Project 2015-04 Alignment of Terms		11/5/2015	1/21/2016	7/1/2016	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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Transmission Reliability Margin	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 ATC/TTC/AFC and CBM/TRM Revisions		8/22/2008	11/24/2009		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	Version 0 Reliability Standards		2/8/2005	3/16/2007		Services provided to the Transmission Customer by the Transmission Service Provider to move energy from a Point of Receipt to a Point of Delivery.
Transmission Service Provider	Project 2015-04 Alignment of Terms	TSP	11/5/2015	1/21/2016	7/1/2016	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 Undervoltage Load Shedding & Underfrequency Load Shedding	UVLS Program	11/13/2014	11/19/2015	4/1/2017	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 Transmission Vegetation Management		2/7/2006	3/16/2007		All plant material, growing or not, living or dead.
Vegetation Inspection	Project 2010-07		5/9/2012	3/21/2013	7/1/2014	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	Version 0 Reliability Standards		2/8/2005	3/16/2007		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 FAC Order 729		1/24/2011	11/17/2011		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

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Adjacent Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007		9/30/2014	A Balancing Authority Area that is interconnected another Balancing Authority Area either directly or via a multi-party agreement or transmission tariff.
Adverse Reliability Impact	Project 2006-06		8/4/2011	NERC withdrew the related petition 3/18/2015.			The impact of an event that results in Bulk Electric System instability or Cascading.
Area Control Error	Version 0 Reliability Standards	ACE	2/8/2005	3/16/2007		3/31/2014	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias and correction for meter error.
Arranged Interchange	Coordinate Interchange		5/2/2006	3/16/2007		9/30/2014	The state where the Interchange Authority has received the Interchange information (initial or revised).
ATC Path	Project 2006-07		8/22/2008	Not approved; Modification directed 11/24/2009			Any combination of Point of Receipt and Point of Delivery for which ATC is calculated; and any Posted Path. (See 18 CFR 37.6(b)(1))
Automatic Generation Control	Version 0 Reliability Standards	AGC	2/8/2005	3/16/2007		12/31/2018	Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the Balancing Authority's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.
Available Transfer Capability	Version 0 Reliability Standards	ATC	2/8/2005	3/16/2007			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.
Balancing Authority	Version 0 Reliability Standards	BA	2/8/2005	3/16/2007		12/31/2018	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
BES Cyber Asset	Project 2008-06		11/26/2012	11/22/2013		6/30/2016	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 equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)
Blackstart Capability Plan	Version 0 Reliability Standards		2/8/2005	3/16/2007		7/1/2013 Will be retired when EOP-005-2 becomes enforceable	A documented procedure for a generating unit or station to go from a shutdown condition to an operating condition delivering electric power without assistance from the electric system. This procedure is only a portion of an overall system restoration plan.
Blackstart Resource	Project 2006-03		8/5/2009	3/17/2011		6/30/2016	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.
Bulk Electric System	Version 0 Reliability Standards	BES	2/8/2005	3/16/2007		6/30/2014	As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Bulk Electric System (Continued)	Project 2010-17	BES	1/18/2012	6/14/2013		Replaced by BES definition FERC approved 3/20/2014	<p>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.</p> <p>Exclusions:</p> <ul style="list-style-type: none"> • E1 - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: <ul style="list-style-type: none"> a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusion I3, 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 Inclusion I3, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating). <p>Note – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion.</p>
Bulk Electric System (Continued)	Project 2010-17	BES	1/18/2012	6/14/2013		Replaced by BES definition FERC approved 3/20/2014	<ul style="list-style-type: none"> • 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 or above 100 kV but 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 customer Load and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following:
Bulk Electric System (Continued)	Project 2010-17	BES	1/18/2012	6/14/2013		Replaced by BES definition FERC approved 3/20/2014	<ul style="list-style-type: none"> a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusion I3 and do not have an aggregate capacity of non-retail generation greater than 75 MVA (gross nameplate rating); b) 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 a monitored Facility 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 Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL). • E4 – Reactive Power devices owned and operated by the retail customer solely for its own use. Note - Elements may be included or excluded on a case-by-case basis through the Rules of Procedure exception process.
Bulk Electric System (FERC issued an order on April 18, 2013 approving the revised definition with an effective date of July 1, 2013. On June 14, 2013, FERC granted NERC’s request to extend the effective date of the revised definition of the Bulk Electric System to July 1, 2014.)	Project 2010-17	BES	1/18/2012	6/14/2013		Replaced by BES definition FERC approved 3/20/2014	<p>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.</p> <p>Inclusions:</p> <ul style="list-style-type: none"> • I1 - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded under Exclusion E1 or E3. • I2 - Generating resource(s) with gross individual nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above. • I3 - Blackstart Resources identified in the Transmission Operator’s restoration plan. • I4 - Dispersed power producing resources with aggregate capacity greater than 75 MVA (gross aggregate nameplate rating) utilizing a system designed primarily for aggregating capacity, connected at a common point at a voltage of 100 kV or above.
Bulk-Power System	Project 2012-08.1 Phase 1		5/9/2013	7/9/2013		6/30/2016	<p>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.</p>

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Business Practices	Project 2006-07		8/22/2008	Not approved; Modification directed			Those business rules contained in the Transmission Service Provider’s applicable tariff, rules, or procedures; associated Regional Reliability Organization or regional entity business practices; or NAESB Business Practices.
Cascading	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	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.
Cascading Outages	Determine Facility Ratings, Operating Limits, and Transfer Capabilities		11/17/2006 Withdrawn 2/12/2008			FERC Remanded 12/27/2007	The uncontrolled successive loss of Bulk Electric System Facilities triggered by an incident (or condition) at any location resulting in the interruption of electric service that cannot be restrained from spreading beyond a predetermined area.
Confirmed Interchange	Coordinate Interchange		5/2/2006	3/16/2007			The state where the Interchange Authority has verified the Arranged Interchange.
Contingency Reserve	Version 0 Reliability Standards		2/8/2005	3/16/2007		12/31/2017	The provision of capacity deployed by the Balancing Authority to meet the Disturbance Control Standard (DCS) and other NERC and Regional Reliability Organization contingency requirements.
Critical Assets	Cyber Security (Permanent)		5/2/2006	1/18/2008		6/30/2016	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Critical Cyber Assets	Cyber Security (Permanent)		5/2/2006	1/18/2008		6/30/2016	Cyber Assets essential to the reliable operation of Critical Assets.
Cyber Assets	Cyber Security (Permanent)		5/2/2006	1/18/2008		6/30/2016	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Security Incident	Cyber Security (Permanent)		5/2/2006	1/18/2008		6/30/2016	Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Cyber Security Incident	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	12/31/2020	A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.
Demand-Side Management	Version 0 Reliability Standards	DSM	2/8/2005	3/16/2007		6/30/2016	The term for all activities or programs undertaken by Load-Serving Entity or its customers to influence the amount or timing of electricity they use.
Distribution Provider	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	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.
Dynamic Interchange Schedule or Dynamic Schedule	Version 0 Reliability Standards		2/8/2005	3/16/2007		9/30/2014	A telemetered reading or value that is updated in real time and used as a schedule in the AGC/ACE equation and the integrated value of which is treated as a schedule for interchange accounting purposes. Commonly used for scheduling jointly owned generation to or from another Balancing Authority Area.
Electronic Security Perimeter	Cyber Security (Permanent)	ESP	5/2/2006	1/18/2008		6/30/2016	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Element	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.
Energy Emergency	Version 0 Reliability Standards		2/8/2005	3/16/2007		3/31/2017	A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers’ expected energy requirements.
Flowgate	Version 0 Reliability Standards		2/8/2005	3/16/2007			A designated point on the transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions.
Frequency Bias Setting	Version 0 Reliability Standards		2/8/2005	3/16/2007		3/31/2015	A value, usually expressed in MW/0.1 Hz, set into a Balancing Authority ACE algorithm that allows the Balancing Authority to contribute its frequency response to the Interconnection.
Generator Operator		GOP	2/8/2005	3/16/2007		6/30/2016	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
Generator Owner		GO	2/8/2005	3/16/2007		6/30/2016	Entity that owns and maintains generating units.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Interchange Authority		IA	5/2/2006	3/16/2007		6/30/2016	The responsible entity that authorizes implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes.
Interconnected Operations Service	Version 0 Reliability Standards		2/8/2005	3/16/2007			A service (exclusive of basic energy and transmission services) that is required to support the reliable operation of interconnected Bulk Electric Systems.
Interconnection	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	When capitalized, any one of the three major electric system networks in North America: Eastern, Western, and ERCOT.
Interconnection	Project 2010-14.1 Phase 1		8/15/2013	4/16/2015			When capitalized, any one of the four major electric system networks in North America: Eastern, Western, ERCOT and Quebec.
Interconnection Reliability Operating Limit	Version 0 Reliability Standards	IROL	2/8/2005	3/16/2007		12/27/2007	The value (such as MW, MVar, Amperes, Frequency or Volts) derived from, or a subset of the System Operating Limits, which if exceeded, could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages.
Intermediate Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007			A Balancing Authority Area that has connecting facilities in the Scheduling Path between the Sending Balancing Authority Area and Receiving Balancing Authority Area and operating agreements that establish the conditions for the use of such facilities.
Load-Serving Entity	Version 0 Reliability Standards		2/8/2005	3/16/2007			Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.
Low Impact BES Cyber System Electronic Access Point	Project 2014-02	LEAP	2/12/2015	1/21/2016	7/1/2016	12/31/2019	A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Low Impact External Routable Connectivity	Project 2014-02	LERC	2/12/2015	1/21/2016	7/1/2016	12/31/2019	Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).
Misoperation	Phase III - IV Planning Standards - Archive		2/7/2006	3/16/2007		6/30/2016	<ul style="list-style-type: none"> Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection. Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone). Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity.
Operational Planning Analysis	Operate Within Interconnection Reliability Operating Limits		10/17/2008	3/17/2011		9/30/2014	An analysis of the expected system conditions for the next day's operation. (That analysis may be performed either a day ahead or as much as 12 months ahead.) Expected system conditions include things such as load forecast(s), generation output levels, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.).
Operational Planning Analysis	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	12/31/2016	An analysis of the expected system conditions for the next day's operation. (That analysis may be performed either a day ahead or as much as 12 months ahead.) Expected system conditions include things such as load forecast(s), generation output levels, Interchange, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.).
Physical Security Perimeter	Cyber Security (Permanent)	PSP	5/2/2006	1/18/2008		6/30/2016	The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.
Planning Authority	Version 0 Reliability Standards	PA	2/8/2005	3/16/2007			The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
Point of Receipt	Version 0 Reliability Standards	POR	2/8/2005	3/16/2007		6/30/2016	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.
Postback	Project 2006-07 ATC/TTC/AFC and CBM/TRM		8/22/2008	Not approved; Modification directed			Positive adjustments to ATC or AFC as defined in Business Practices. Such Business Practices may include processing of redirects and unscheduled service.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Protected Cyber Assets	Project 2008-06 Cyber Security Order 706	PCA	11/26/2012	11/22/2013		6/30/2016	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. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Protection System	Phase III-IV Planning Standards - Archive		2/7/2006	3/17/2007		4/1/2013	Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.
Protection System Maintenance Program (PRC-005-2)	Project 2007-17 Protection System Maintenance and Testing	PSMP	11/7/2012	12/19/2013		4/1/2015	An ongoing program by which Protection System 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.
Protection System Maintenance Program (PRC-005-3)	Project 2007-17.2 Protection System Maintenance and Testing - Phase 2	PSMP	11/7/2013	1/22/2015	4/1/2016		An ongoing program by which Protection System and automatic reclosing 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.
Protection System Maintenance Program (PRC-005-4)	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PSMP	11/13/2014	9/17/2015	1/1/2016		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	Version 0 Reliability Standards		2/8/2005	3/16/2007			A telemetered reading or value that is updated in real time and used as a “virtual” tie line flow in the AGC/ACE equation but for which no physical tie or energy metering actually exists. The integrated value is used as a metered MWh value for interchange accounting purposes.
Pseudo-Tie	Project 2008-12		2/6/2014	6/30/2014	10/1/2014	12/31/2018	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’ control ACE equations (or alternate control processes).
Reactive Power	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	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	Version 0 Reliability Standards		2/8/2005	3/16/2007			The portion of electricity that supplies energy to the load.
Reallocation	Version 0 Reliability Standards		2/8/2005	3/16/2007			The total or partial curtailment of Transactions during TLR Level 3a or 5a to allow Transactions using higher priority to be implemented.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Real-time Assessment	Project 2014-03		11/13/2014	Revised definition. 11/19/2015	1/1/2017	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 Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)	
Real-time Assessment	Operate Within Interconnection Reliability Operating Limits		10/17/2008	3/17/2011		12/31/2016	An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data
Reliability Coordinator	Version 0 Reliability Standards	RC	2/8/2005	3/16/2007		6/30/2007	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 Directive	Project 2006-06 Reliability Coordination		8/16/2012	11/19/2015		11/19/2015	A communication initiated by a Reliability Coordinator, Transmission Operator, or Balancing Authority where action by the recipient is necessary to address an Emergency or Adverse Reliability Impact.
Reliability Standard	Project 2012-08.1 Phase 1 of Glossary Updates: Statutory Definitions		5/9/2013	7/9/2013		6/30/2016	A requirement, approved by the United States Federal Energy Regulatory Commission under this Section 215 of the Federal Power Act, or approved or recognized by an applicable governmental authority in other jurisdictions, to provide for reliable operation [Reliable Operation] of the bulk-power system [Bulk-Power System]. The term includes requirements for the operation of existing bulk-power system [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 [Reliable Operation] of the bulk-power system [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 2012-08.1 Phase 1 of Glossary Updates: Statutory Definitions		5/9/2013	7/9/2013		6/30/2016	Operating the elements of the bulk-power system [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	Version 0 Reliability Standards	RAS	2/8/2005	3/16/2007		3/31/2017	See "Special Protection System"
Removable Media	Project 2014-02		2/12/2015	1/21/2016	7/1/2016	12/31/2019	Storage media that (i) are not Cyber Assets, (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, a network within an ESP, or a Protected Cyber Asset. Examples 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.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Reporting Ace			8/15/2013	4/16/2015 (Will not go into effect)			<p>The scan rate values of a Balancing Authority’s Area Control Error (ACE) measured in MW, which includes the difference between the Balancing Authority’s Net Actual Interchange and its Net Scheduled Interchange, plus its Frequency Bias obligation, plus any known meter error. In the Western Interconnection, Reporting ACE includes Automatic Time Error Correction (ATEC).</p> <p>Reporting ACE is calculated as follows: Reporting ACE = (NI_A – NI_S) – 10B (F_A – F_S) – I_{ME} 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) is the algebraic sum of actual megawatt transfers across all Tie Lines and includes Pseudo-Ties. Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude megawatt transfers on those Tie lines in their actual interchange, provided they are implemented in the same manner for Net Interchange Schedule. NI_S (Scheduled Net Interchange) is the algebraic sum of all scheduled megawatt transfers, including Dynamic Schedules, with adjacent Balancing Authorities, and taking into account the effects of schedule ramps. Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude megawatt transfers on those Tie Lines in their scheduled Interchange, provided they are implemented in the same manner for Net Interchange Actual.</p>
Reporting Ace (Continued)			8/15/2013	4/16/2015 (Will not go into effect)			<p>B (Frequency Bias Setting) is the Frequency Bias Setting (in negative MW/0.1 Hz) for the Balancing Authority. 10 is the constant factor that converts the frequency bias setting units to MW/Hz. F_A (Actual Frequency) is the measured frequency in Hz. F_S (Scheduled Frequency) is 60.0 Hz, except during a time correction. I_{ME} (Interchange Meter Error) is the meter error correction factor and represents the difference between the integrated hourly average of the net interchange actual (NIA) and the cumulative hourly net Interchange energy measurement (in megawatt-hours). I_{ATEC} (Automatic Time Error Correction) is 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.</p> <p>ATEC shall be zero when operating in any other AGC mode.</p> <ul style="list-style-type: none">• Y = B / BS.• H = Number of hours used• BS = Frequency Bias for the <p>$I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)^H}$ when operating in Automatic Time Error Correction control mode. rgy. The value of H is set to 3.</p>
Reporting Ace (Continued)							<p>energy. The value of H is set to 3. B_S = Frequency Bias for the Interconnection (MW / 0.1 Hz).</p> <ul style="list-style-type: none">• Primary Inadvertent Interchange (PII_{hourly}) is (1-Y) * (II_{actual} - B * ΔTE/6)• 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:ΔTE = 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’s accumulated PII_{hourly} in MWh. An On-Peak and Off-Peak accumulation accounting is required. <p>Where:</p> <p>$PII_{accum}^{on/off\ peak} = \text{last period's } PII_{accum}^{on/offpeak} + PII_{hourly}$</p> <p>All NERC Interconnections with multiple Balancing Authorities 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 equation that is(are) implemented for all BAs on an Interconnection and is(are) consistent with the following four principles will provide a valid alternative Reporting ACE equation</p>

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Reporting Ace (Continued)			8/15/2013	4/16/2015 (Will not go into effect)			<p>All NERC Interconnections with multiple Balancing Authorities 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 equation that is(are) implemented for all Balancing Authorities on an interconnection and is(are) consistent with the following four principles will provide a valid alternative Reporting ACE equation consistent with the measures included in this standard.</p> <ol style="list-style-type: none"> 1. All portions of the Interconnection are included in one area or another so that the sum of all area generation, loads and losses is the same as total system generation, load and losses. 2. The algebraic sum of all area Net Interchange Schedules and all Net Interchange actual values is equal to zero at all times. 3. The use of a common Scheduled Frequency FS for all areas at all times. 4. The absence of metering or computational errors. (The inclusion and use of the IME term to account for known metering or computational errors.)
Reportable Cyber Security Incident	Project 2008-06 Cyber Security Order 706 V5 CIP Standards		11/26/2012	11/22/2013	7/1/2016	12/31/2020	A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.
Request for Interchange	Coordinate Interchange	RFI	5/2/2006	3/16/2007			A collection of data as defined in the NAESB RFI Datasheet, to be submitted to the Interchange Authority for the purpose of implementing bilateral Interchange between a Source and Sink Balancing Authority.
Reserve Sharing Group	Version 0 Reliability Standards	RSG	2/8/2005	3/16/2007		6/30/2016	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 quicker (e.g., between zero and ten minutes) then, for the purposes of Disturbance Control Performance, the Areas become a Reserve Sharing Group.
Reserve Sharing Group Reporting ACE	Project 2010-14.1 Phase 1		8/15/2013	4/16/2015		12/31/2017	At any given time of measurement for the applicable Reserve Sharing Group, the algebraic sum of the Reporting ACEs (or equivalent as calculated at such time of measurement) of the Balancing Authorities participating in the Reserve Sharing Group at the time of measurement.
Resource Planner	Version 0 Reliability Standards	RP	2/8/2005	3/16/2007			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.
Right-of-Way	Project 2007-07	ROW	2/7/2006	3/16/2007			A corridor of land on which electric lines may be located. The Transmission Owner may own the land in fee, own an easement, or have certain franchise, prescription, or license rights to construct and maintain lines.
Right-of-Way	Project 2007-07	ROW	11/3/2011	3/21/2013		6/30/2014	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 Transmission Owner's legal rights but may be less based on the aforementioned criteria.
Sink Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007		9/30/2014	The Balancing Authority in which the load (sink) is located for an Interchange Transaction. (This will also be a Receiving Balancing Authority for the resulting Interchange Schedule.)
Source Balancing Authority	Version 0 Reliability Standards		2/8/2005	3/16/2007		9/30/2014	The Balancing Authority in which the generation (source) is located for an Interchange Transaction. (This will also be a Sending Balancing Authority for the resulting Interchange Schedule.)
Special Protection System (Remedial Action Scheme)	Version 0 Reliability Standards	SPS	2/8/2005	3/16/2007 (Becomes inactive 3/31/2017)		3/31/2017	An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme.

Retired Terms							
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
System Operating Limit	Version 0 Reliability Standards	SOL	2/8/2005	3/16/2007		6/30/2014	The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: <ul style="list-style-type: none"> • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)
System Operator	Version 0 Reliability Standards		2/8/2005	3/16/2007		6/30/2016	An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.
Transient Cyber Asset	Project 2014-02		2/12/2015	1/21/2016	7/1/2016		A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is 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, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Transmission Customer	Version 0 Reliability Standards		2/8/2005	3/16/2007			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 responsible entities: Generator Owner, Load-Serving Entity, or Purchasing-Selling Entity.
Transmission Operator	Version 0 Reliability Standards	TOP	2/8/2005	3/16/2007			The entity responsible for the reliability of its “local” transmission system, and that operates or directs the operations of the transmission facilities.
Transmission Owner	Version 0 Reliability Standards	TO	2/8/2005	3/16/2007			The entity that owns and maintains transmission facilities.
Transmission Planner	Version 0 Reliability Standards	TP	2/8/2005	3/16/2007			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 Service Provider	Version 0 Reliability Standards	TSP	2/8/2005	3/16/2007			The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
Vegetation Inspection	Project 2007-07 Transmission Vegetation Management		2/7/2006	3/16/2007		3/20/2013	The systematic examination of a transmission corridor to document vegetation conditions.
Vegetation Inspection	Project 2007-07 Transmission Vegetation Management		11/3/2011	3/21/2013		6/30/2014	The systematic examination of vegetation conditions on a Right-of-Way and those vegetation conditions under the Transmission 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.

NPCC REGIONAL DEFINITIONS							
NPCC 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							
RELIABILITYFIRST Regional Term	Link to FERC Order	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			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			Total of all end-use customer demand and electric system losses within specified metered boundaries, less Direct Control Management and Interruptible Demand
Peak Period	BAL-502-RFC-02 Implementation Plan		8/5/2009	3/17/2011			A period consisting of two (2) or more calendar months but less than seven (7) calendar months, which includes the period during which the responsible entity's annual peak demand is expected to occur
Wind Generating Station	BAL-502-RFC-02 Implementation Plan		11/3/2011 (Board withdrew approval 11/7/2012)	3/17/2011			A collection of wind turbines electrically connected together and injecting energy into the grid at one point, sometimes known as a "Wind Farm."
Year One	BAL-502-RFC-02 Implementation Plan		8/5/2009	3/17/2011			The planning year that begins with the upcoming annual Peak Period

TEXAS RE REGIONAL DEFINITIONS

Frequency Measurable Event	BAL-001-TRE-1 Implementation Plan	FME	8/15/2013	1/16/2014	4/1/2014	<p>An event that results in a Frequency Deviation, identified at the BA's sole discretion, and meeting one of the following conditions:</p> <p>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).</p> <p>Or</p> <p>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).</p>
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							
WECC Regional Term	WECC Standards Under Development	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Area Control Error *	WECC Regional Standards Under Development	ACE	3/12/2007	6/8/2007		3/31/2014	Means the instantaneous difference between net actual and scheduled interchange, taking into account the effects of Frequency Bias including correction for meter error.
Automatic Generation Control *	WECC Regional Standards Under Development	AGC	3/12/2007	6/8/2007			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		3/26/2008	5/21/2009		3/31/2014	A frequency control automatic action that a Balancing Authority uses to offset its frequency contribution to support the Interconnection's scheduled frequency.
Automatic Time Error Correction	WECC Regional Standards Under Development		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.
Average Generation *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means the total MWh generated within the Balancing Authority Operator's Balancing Authority Area during the prior year divided by 8760 hours (8784 hours if the prior year had 366 days).
Business Day *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means any day other than Saturday, Sunday, or a legal public holiday as designated in section 6103 of title 5, U.S. Code.

Commercial Operation	WECC Regional Standards Under Development		10/29/2008	4/21/2011			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.
Contributing Schedule	WECC Regional Standards Under Development		2/10/2009	3/17/2011		9/30/2019	A Schedule not on the Qualified Transfer Path between a Source Balancing Authority and a Sink Balancing Authority that contributes unscheduled flow across the Qualified Transfer Path.
Dependability-Based Misoperation	WECC Regional Standards Under Development		10/29/2008	4/21/2011			Is the absence of a Protection System or RAS operation when intended. Dependability is a component of reliability and is the measure of a device's certainty to operate when required.
Disturbance *	WECC Regional Standards Under Development		3/12/2007	6/8/2007		Retired	Means (i) any perturbation to the electric system, or (ii) the unexpected change in ACE that is caused by the sudden loss of generation or interruption of load.
Extraordinary Contingency†	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Shall have the meaning set out in Excuse of Performance, section B.4.c. language in section B.4.c: <i>means any act of God, actions by a non-affiliated third party, labor disturbance, act of the public enemy, war, insurrection, riot, fire, storm or flood, earthquake, explosion, accident to or breakage, failure or malfunction of machinery or equipment, or any other cause beyond the Reliability Entity's reasonable control; provided that prudent industry standards (e.g. maintenance, design, operation) have been employed; and provided further that no act or cause shall be considered an Extraordinary Contingency if such act or cause results in any contingency contemplated in any WECC Reliability Standard (e.g., the "Most Severe Single Contingency" as defined in the WECC Reliability Criteria or any lesser contingency).</i>

WECC REGIONAL DEFINITIONS							
WECC Regional Term	WECC Standards Under Development	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition
Frequency Bias *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means a value, usually given in megawatts per 0.1 Hertz, associated with a Control Area that relates the difference between scheduled and actual frequency to the amount of generation required to correct the difference.
Functionally Equivalent Protection System	WECC Regional Standards Under Development	FEPS	10/29/2008	4/21/2011			A Protection System that provides performance as follows: <ul style="list-style-type: none"> • Each Protection System can detect the same faults within the zone of protection and provide the clearing times and coordination needed to comply with all Reliability Standards. • Each Protection System may have different components and operating characteristics.

Functionally Equivalent RAS	WECC Regional Standards Under Development	FERAS	10/29/2008	4/21/2011			A Remedial Action Scheme (“RAS”) that provides the same performance as follows: • Each RAS can detect the same conditions and provide mitigation to comply with all Reliability Standards. • Each RAS may have different components and operating characteristics.
Generating Unit Capability *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means the MVA nameplate rating of a generator.
Non-spinning Reserve†	WECC Regional Standards Under Development		3/12/2007	6/8/2007		Retired	Means that Operating Reserve not connected to the system but capable of serving demand within a specified time, or interruptible load that can be removed from the system in a specified time.
Normal Path Rating *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Is the maximum path rating in MW that has been demonstrated to WECC through study results or actual operation, whichever is greater. For a path with transfer capability limits that vary seasonally, it is the maximum of all the seasonal values.
Operating Reserve *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means that capability above firm system demand required to provide for regulation, load-forecasting error, equipment forced and scheduled outages and local area protection. Operating Reserve consists of Spinning Reserve and Nonspinning Reserve.
Operating Transfer Capability Limit *	WECC Regional Standards Under Development	OTC	3/12/2007	6/8/2007			Means the maximum value of the most critical system operating parameter(s) which meets: (a) precontingency criteria as determined by equipment loading capability and acceptable voltage conditions, (b) transient criteria as determined by equipment loading capability and acceptable voltage conditions, (c) transient performance criteria, and (d) post-contingency loading and voltage criteria
Primary Inadvertent Interchange	WECC Regional Standards Under Development		3/26/2008	5/21/2009			The component of area (n) inadvertent interchange caused by the regulating deficiencies of the area (n).
Qualified Controllable Device	WECC Regional Standards Under Development		2/10/2009	3/17/2011		9/30/2019	A controllable device installed in the Interconnection for controlling energy flow and the WECC Operating Committee has approved using the device for controlling the USF on the Qualified Transfer Paths.
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).
Qualified Transfer Path	WECC Regional Standards Under Development		2/10/2009	3/17/2011		9/30/2019	A transfer path designated by the WECC Operating Committee as being qualified for WECC unscheduled flow mitigation.
Qualified Transfer Path Curtailment Event	WECC Regional Standards Under Development		2/10/2009	3/17/2011		9/30/2019	Each hour that a Transmission Operator calls for Step 4 or higher for one or more consecutive hours (See Attachment 1 IRO-006-WECC-1) during which the curtailment tool is functional.
WECC REGIONAL DEFINITIONS							
WECC Regional Term	WECC Standards Under Development	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Inactive Date	Definition

Relief Requirement	WECC Regional Standards Under Development		2/10/2009	3/17/2011		6/30/2014	The expected amount of the unscheduled flow reduction on the Qualified Transfer Path that would result by curtailing each Sink Balancing Authority's Contributing Schedules by the percentages listed in the columns of WECC Unscheduled Flow Mitigation Summary of Actions Table in Attachment 1 WECC IRO-006-WECC-1.
Relief Requirement	WECC Regional Standards Under Development		2/7/2013	6/13/2014	7/1/2014	9/30/2019	The expected amount of the unscheduled flow reduction on the Qualified Transfer Path that would result by curtailing each Sink Balancing Authority's Contributing Schedules by the percentages determined in the WECC unscheduled flow mitigation guideline.
Secondary Inadvertent Interchange	WECC Regional Standards Under Development		3/26/2008	5/21/2009			The component of area (n) inadvertent interchange caused by the regulating deficiencies of area (i).
Security-Based Misoperation	WECC Regional Standards Under Development		10/29/2008	4/21/2011			A Misoperation caused by the incorrect operation of a Protection System or RAS. Security is a component of reliability and is the measure of a device's certainty not to operate falsely.
Spinning Reserve [†]	WECC Regional Standards Under Development		3/12/2007	6/8/2007		Retired	Means unloaded generation which is synchronized and ready to serve additional demand. It consists of Regulating reserve and Contingency reserve (as each are described in Sections B.a.i and ii).
Transfer Distribution Factor	WECC Regional Standards Under Development	TDF	2/10/2009	3/17/2011		9/30/2019	The percentage of USF that flows across a Qualified Transfer Path when an Interchange Transaction (Contributing Schedule) is implemented. [See the WECC Unscheduled Flow Mitigation Summary of Actions Table (Attachment 1 WECC IRO-006-WECC-1).]
WECC Table 2 *	WECC Regional Standards Under Development		3/12/2007	6/8/2007			Means the table maintained by the WECC identifying those transfer paths monitored by the WECC regional Reliability coordinators. As of the date set out therein, the transmission paths identified in Table 2 are as listed in Attachment A to this Standard.

[†] FERC approved the WECC Tier One Reliability Standards in the Order Approving Regional Reliability Standards for the Western Interconnection and Directing Modifications, 119 FERC ¶ 61,260 (June 8, 2007). In that Order, FERC directed WECC to address the inconsistencies between the regional definitions and the NERC Glossary in developing permanent replacement standards. The replacement standards designed to address the shortcomings were filed with FERC in 2009.

CHANGE HISTORY	
Date	Action
4/2/2021	Retired;moved to the Retired Terms Tab: Reportable Cyber Security Incident
3/31/2021	Retired; moved to the Retired Terms tab: 1. Operational Planning Analysis (OPA), 2. Protections System Coordination Study 3. Real-time Assessment (RTA)
3/15/2021	Moved; to Subject to Enforcement Tab 1. Operational Planning Analysis (OPA) 2. 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. 1. Automatic Generation Control 2. 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: 1. Definition of Transient Cyber Asset (TCA) 2. Definition of Removable Media
1/2/2020	Retired; moved to the Retired Terms tab. 1. Low Impact BES Cyber System Electronic Access Point (LEAP) 2. Low Impact External Routable Connectivity (LERC) 3. 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 Media link to project 2014-02.
7/3/2017	Moved 'Geomagnetic Disturbance Vulnerability Assessment or GMD Vunerability Assessment' to Subject to Enforcement
6/15/2017	Readded 'Governor' and 'Primary Frequency Response' to TexasRE
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