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

North American Electric	**)**
Reliability Corporation	**)**

FOURTH QUARTER 2018 APPLICATION FOR APPROVAL OF RELIABILITY STANDARDS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Shamai Elstein
Assistant General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

February 28, 2019

TABLE OF CONTENTS

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

North American Electric	**)**
Reliability Corporation	**)**

FOURTH QUARTER 2018 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 the following NERC Reliability Standards approved by the United States Federal Energy Regulatory Commission ("FERC") during the fourth quarter of 2018 (from October 1, 2018 through December 31, 2018): CIP-005-6, CIP-010-3, CIP-013-1, PER-003-2, and VAR-001-5.

NERC also requests approval of proposed Reliability Standard TPL-007-3 (Transmission System Planned Performance for Geomagnetic Disturbance Events) and its associated implementation plan. As discussed further below, a prior version of the TPL-007 standard, TPL-007-2, was approved by FERC in the fourth quarter of 2018. As TPL-007-2 has since been superseded by TPL-007-3, which modifies the TPL-007 standard by including a new Variance for Canadian registered entities, NERC is submitting proposed Reliability Standard TPL-007-3 for approval. As the new Variance in proposed Reliabilty Standard TPL-007-3 applies only to Canadian entities, TPL-007-3 is not being filed with FERC for approval.

NERC requests that the Reliability Standards submitted for approval 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, where applicable, of each Reliability Standard

submitted for approval (**Exhibit A-1**); (ii) an informational summary of each Reliability Standard submitted for approval, including the standard's purpose, applicability, and, where applicable, 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 submitted for approval (**Exhibit A-3**); (iv) the implementation plan for proposed Reliability Standard TPL-007-3 (**Exhibit A-4**); (v) an updated list of the currently effective NERC Reliability Standards as approved by FERC (**Exhibit B**); and (vi) 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:

Shamai Elstein
Assistant General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@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 was certified by the

[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) (2018) (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).

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.[4] Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to FERC-approved Reliability Standards.[5] Section 215(d)(5) of the FPA authorizes FERC to order the ERO to submit a new or modified Reliability Standard and Section 39.5(a) of FERC's regulations requires the ERO to file for FERC approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective in the United States.[6]

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,[7] and a separate MOU with Nova Scotia Power Incorporated ("NSPI") and the Northeast Power Coordinating Council, Inc. ("NPCC"),[8] 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

---

3 *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing,* 116 FERC ¶ 61,062 (2006), *order on reh'g and compliance,* 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa Inc. v. FERC,* 564 F.3d 342 (D.C. Cir. 2009).

4 16 U.S.C. § 824o.

5 *Id*. § 824o(b)(1).

6 *Id*. § 824o(d)(5).

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

8 *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).

improve the reliability of the North American BPS. The May 11, 2010 MOU sets forth the mutual understandings 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. On July 20, 2011, NSUARB issued a decision approving these documents. [9] In that decision, the NSUARB approved a "quarterly review" process for considering new and amended NERC Reliability Standards and criteria[10] and ordered that "applications will not be processed by the Board until [FERC] has approved or remanded the standards in the United States."[11] 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.[12]

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

---

9 *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) ("NSUARB Decision").

10 *Id*. at P 30.

11 *Id*.

12 *Id*. at P 33.

associated with NERC Reliability Standards.[13] 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.

B. Overview of NERC Reliability Standards Development Process

NERC Reliability Standards define the requirements for reliably planning and operating the North American BPS. These standards are developed by industry stakeholders using a balanced, open, fair, and inclusive process managed by the NERC Standards Committee. The Standards Committee is facilitated by NERC staff and comprised of representatives from ten electricity stakeholder segments. Stakeholders, through a balloting process, approve the Reliability 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 (Standards Processes Manual) of its Rules of Procedure.[14] 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 July 3, 2018, 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.

---

[13] NERC's VRF Matrix and VSL Matrix are available at: http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United States. *See* left-hand side of webpage for downloadable documents.

[14] The NERC *Rules of Procedure* are available at: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

C. Description of Proposed Reliability Standards

As provided in the table below, during the fourth quarter of 2018, FERC issued four orders approving the following Reliability Standards: (i) VAR-001-5;[15] (ii) CIP-005-6, CIP-010-3 and CIP-013-1;[16] (iii) TPL-007-2;[17] and (iv) PER-003-2.[18] No other Reliability Standards or definitions were approved during the fourth quarter of 2018.

Reliability Standards	Effective Dates
Critical Infrastructure Protection (CIP) Standards	
CIP-005-6*	7/1/2020
CIP-010-3*	7/1/2020
CIP-013-1*	7/1/2020
Personnel Performance, Training, and Qualifications (PER) Standard	
PER-003-2*	7/1/2019
Transmission Planning (TPL) Standard	
TPL-007-2*	7/1/2019
Voltage and Reactive (VAR) Standard	
VAR-001-5	1/1/2019

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

As discussed further below, the NERC Board of Trustees has since adopted proposed Reliability Standard TPL-007-3, which supersedes TPL-007-2. As proposed Reliability Standard TPL-007-3 was modified to include a Variance for Canadian registered entities and will not be filed for FERC approval, NERC submits proposed Reliability Standard TPL-007-3 for NSUARB approval in this filing.

1. *CIP-005-6, CIP-010-3, and CIP-013-1*

On October 18, 2018, FERC issued a final rule approving: (i) Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security –

---

15 *N. Am. Elec. Reliability Corp.*, Docket No. RD18-8-000 (Oct. 15, 2018) (delegated letter order).

16 *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018).

17 *Geomagnetic Disturbance Reliability Standard; Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*, Order No. 851, 165 FERC ¶ 61,124 (2018).

18 *N. Am. Elec. Reliability Corp.*, Docket No. RD18-9-000 (Nov. 21, 2018) (delegated letter order).

Electronic Security Perimeter(s)), and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments).; (ii) the associated Implementation Plan; (iii) the associated VRFs and VSLs; and (iv) the retirement of currently-effective Reliability Standards CIP-005-5 and CIP-010-2.

The Reliability Standards are designed to augment the existing controls required in the currently-effective Critical Infrastructure Protection ("CIP") Reliability Standards that help mitigate supply chain risks, providing increased attention on minimizing the attack surfaces of information and communications technology products and services procured to support reliable Bulk Electric System operations, consistent with Order No. 829.[19]

Specifically, Reliability Standard CIP-013-1 improves reliability by requiring Responsible Entities to implement processes to: (1) identify and assess cybersecurity risks to the BES from vendor products and services in their planning activities for high and medium impact BES Cyber Systems; and (2) include specified security concepts in their procurement activities for high and medium impact BES Cyber Systems. Modifications in Reliability Standards CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.

2. PER-003-2

On November 21, 2018, FERC issued a delegated order approving revised Reliability Standard PER-003-2 (Operating Personnel Credentials) and the retirement of currently-effective Reliability Standards PER-003-1 and PER-004-2 (Reliability Coordination – Staffing).

[19] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016).

The purpose of Reliability Standard PER-003-2 is designed to ensure that System Operators performing the reliability-related tasks of the Reliability Coordinator, Balancing Authority and Transmission Operator are certified through the NERC System Operator Certification Program when filling a Real-time operating position responsible for control of the Bulk Electric System.

3. TPL-007-3

Reliability Standard TPL-007-1, which is currently enforceable in Nova Scotia, requires applicable entities to conduct initial and ongoing assessments of the potential impact of a 1-in-100 year benchmark geomagnetic disturbance ("GMD") event on Bulk Power System ("BPS") equipment and the BPS as a whole. FERC approved Reliability Standard TPL-007-1 in Order No. 830, issued on September 22, 2016.[20] FERC also directed the following four revisions to the standard to address areas of concern noted in the order and underlying proceeding:

- First, FERC directed NERC to "develop revisions to the benchmark GMD event definition so that the reference peak geoelectric field amplitude component is not based solely on spatially-averaged data."[21]
- Second, FERC directed NERC to revise TPL-007-1 Requirement R6 "to require registered entities to apply spatially averaged and non-spatially averaged peak geoelectric field values, or some equally and efficient alternative, when conducting thermal impact assessments."[22]
- Third, FERC directed NERC to revise TPL-007-1 to require entities "to collect [geomagnetically induced current ("GIC")] monitoring and magnetometer data as necessary to enable model validation and situational awareness, including from any devices that must be added to meet this need."[23]

---

[20] *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*, Order No. 830, 156 FERC ¶ 61,215 (2016), *reh'g denied*, Order No. 830-A, 158 FERC ¶ 61,041 (2017) (Order No. 830).

[21] Order No. 830 at P 44.

[22] *Id*. at P 65.

[23] *Id*. at P 88.

- Fourth, FERC directed NERC to modify TPL-007-1 requirements for Corrective Action Plans to include: (i) a one-year deadline for the development of any necessary Corrective Action Plans; (ii) a two-year deadline for the implementation of non-hardware mitigation; and (iii) a four-year deadline for the implementation of hardware mitigation.[24]

In response to FERC's directives, NERC developed Reliability Standard TPL-007-2. Reliability Standard TPL-007-2 added new Requirements for entities to assess their vulnerabilities to a second defined event, the supplemental GMD event. This supplemental GMD event was designed to account for the localized peak effects of severe GMD events on systems and equipment. The standard also contained new Requirements for the collection of GIC and magnetometer data. Lastly, the standard revised Requirement R7 to include deadlines for the development and completion of any necessary Corrective Action Plans. On November 15, 2018, the FERC issued Order No. 851 approving Reliability Standard TPL-007-2 and issuing directives for further standard modifications.[25]

In early 2018, NERC initiated Project 2018-01 Canadian-specific Revisions to TPL-007-2. The purpose of this project was to consider revisions to the TPL-007-2 standard that would: (i) allow Canadian jurisdictions to define and implement alternative benchmark and supplemental GMD events for performing GMD Vulnerability Assessments; and (ii) account for regulatory approval processes in place in some Canadian jurisdictions to implement capital improvements identified in Corrective Action Plans.

NERC appointed a standard drafting team consisting of subject matter experts from several Canadian provinces to develop a Variance to TPL-007-2. The TPL-007-2 standard with the new Variance was assigned standard version number TPL-007-3 and was posted for comment and ballot. During the final ballot, proposed Reliability Standard TPL-007-3 achieved a

---

[24] *Id*. at PP 101-02.

[25] *Supra* note 17.

100 percent approval rating with 80.43 percent quorum. The associated implementation plan achieved a 100 percent approval rating with 82.09 percent quorum. The NERC Board of Trustees adopted the proposed standard on February 7, 2019.

As provided in Section D.A of Reliability Standard TPL-007-3, the Regional Variance for Canadian Jurisdictions shall apply only to entities in Canada.[26] The applicability of this Variance reflects the substantial work that has been done in Canada to develop regionally specific data that may be used to develop alternative GMD planning events. Recognizing the role of the provincial authorities with respect to Reliability Standards, Section D.A further provides that the Variance shall apply "in those Canadian jurisdictions where the Variance has been approved for use by the applicable governmental authority or has otherwise become effective in the jurisdiction."

Proposed Reliability Standard TPL-007-3 is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standard builds upon the improvements reflected in the prior version of the TPL-007 standard and incorporates a new Variance option for Canadian registered entities. This Variance option maintains the rigor of the continent-wide Requirements by continuing to require entities to assess their vulnerabilities to GMD planning events of a 1-in-100 year severity. The Variance differs from the continent-wide approach in that it allows applicable Canadian entities to use regionally specific data to develop GMD planning events for their planning areas in lieu of the benchmark and supplemental GMD events defined in the standard. The Variance also recognizes some differences in Canadian

[26] NERC is filing proposed Reliability Standard TPL-007-3 for approval with each Canadian jurisdiction; the standard will be filed with FERC for informational purposes only as the modifications therein apply only to entities in Canada.

jurisdictions relating to regulatory approvals for capital investments identified in Corrective Action Plans. The following is additional details on the modifications in TPL-007-3.

Attachment 1-CAN – Proposed Reliability Standard TPL-007-3 contains Requirements for entities to assess their vulnerabilities to two defined GMD events: (i) the benchmark GMD event, intended to assess vulnerabilities to the wide scale impacts of a severe, 1-in-100 year GMD event; and (ii) the supplemental GMD event, intended to account for the effects of localized peaks that could potentially affect reliable operations. These events are described in detail in Attachment 1 to the standard and are referenced in several TPL-007 standard Requirements relating to the different studies and obligations to be performed to develop benchmark and supplemental GMD Vulnerability Assessments.

Under the Variance, all references to "Attachment 1" in the TPL-007-3 Requirements would be replaced with "Attachment 1 or Attachment 1-CAN". Attachment 1-CAN describes an alternative approach that an entity may use to develop alternative benchmark or supplemental GMD event(s) to use in performing its GMD Vulnerability Assessment(s). An entity may use Attachment 1-CAN only where the Variance has been approved for use by the applicable governmental authority or where it has otherwise become effective in the jurisdiction. The alternative benchmark or supplemental GMD event(s) would achieve an equivalent level of reliability as established in the Attachment 1; that is, entities would be required to assess their vulnerabilities to a 1-in-100 year GMD event, including the wide scale and localized impacts of such an event.

NERC has determined that adding an alternative option is appropriate for Canadian entities given the significant advancements in Canada in GMD data collection and research. Geomagnetic observatories have been operating in Canada since the 1840s. Digital data since the

1970s is available, providing a 40-year digital archive for analysis. Work is also underway to digitize the earlier analog records, which would expand the digital archive further. Earth conductivity information has been collected during magnetotelluric studies, particularly as part of the Lithoprobe program.[27] This information has been used to generate a set of earth 1-D conductivity models for the different geologic terrains within each province. In some places, these magnetotelluric studies provide information for producing 2-D and 3-D earth conductivity models.

An extreme value statistics study has been completed using the 1-minute geomagnetic observatory data and earth conductivity models that provides an initial assessment of the 1-in-100 year extreme geomagnetic and geoelectric field values in different parts of Canada.[28] Work is now underway to use data with faster sampling rates (10-second, 5-second, and 1-second) to determine how the faster geomagnetic field variations captured in this data influence the 1-in-100 year results. Ongoing research also allows for more accurate characterization of regional parameters in planning models. For example, work has been conducted to use the growing Canadian data set in the evaluation of earth conductivity model effects to geomagnetically induced current modeling.[29]

The Variance would allow entities to take advantage of available data and ongoing research, such as the examples cited above, to develop customized, 1-in-100 year GMD planning event(s) specific to their planning area. When studied, these customized GMD planning events

---

[27] Lithoprobe – Canada's National Geoscience Project, http://lithoprobe.eos.ubc.ca/.

[28] L. Nikitina et al., *Assessment of Extreme Values in Geomagnetic and Geoelectric Field Variation for Canada*, 14 SPACE WEATHER 481 (2016), https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1002/2016SW001386.

[29] *See* L. Marti et al., *Simulation of Geomagnetically Induced Currents with Piecewise Layered Earth Models*, 29 IEEE TRANSACTIONS ON POWER DELIVERY 1886 (2014).

may provide a more representative depiction of the conditions an entity could expect to experience in its specific planning area during a severe, 1-in-100 year GMD event. The reliability benefit of such an approach is that it would allow an entity to develop a better understanding of the system impacts it is likely to experience during such an event and the types of corrective actions that would best address them.

The approach described in Attachment 1-CAN provides considerations for developing technically justified, alternative GMD planning events, including calculating geoelectric fields using geomagnetic field variations and earth transfer function(s) (i.e., the relationship between the electric fields and magnetic field variations at the surface of the earth). Reflecting the need to study both the potential wide scale and localized impacts of a severe GMD event, Attachment 1-CAN provides that the entity shall consider: (i) the large-scale spatial structure of the GMD event for the benchmark GMD Vulnerability Assessment (Requirement R4); and (ii) the small-scale (i.e. localized) spatial structure of the GMD event for the supplemental GMD Vulnerability Assessment (Requirement R8). Attachment 1-CAN also provides examples of information and data that may be used in developing these alternative GMD planning events.

Importantly, Attachment 1-CAN specifies that an entity may opt to use this alternative approach only where it has regionally specific information that provides a technically justified means to define 1-in-100 year GMD event(s) for its planning area. Entities that do not have sufficient information to develop alternative planning events using the approach described in Attachment 1-CAN must continue to use the benchmark and supplemental GMD events defined in Attachment 1 to perform their GMD Vulnerability Assessments. The benchmark and supplemental GMD events defined in Attachment 1 continue to provide a technically justified

representation of a severe 1-in-100 year GMD event and remain appropriate for use in GMD Vulnerability Assessments.

Variance Requirements for Corrective Action Plans (Requirement R7) – As with currently effective version of the TPL-007 Reliability Standard, proposed Reliability Standard TPL-007-3 Requirement R7 would require entities to develop Corrective Action Plans to address system performance issues for GMD Vulnerability Assessments performed using the benchmark GMD event. Pursuant to FERC Order No. 830[30], certain revisions were made to this Requirement in the previous version of the standard, TPL-007-2. First, Requirement R7 Part 7.2 was revised to provide that the entity shall have one year from the completion of the GMD Vulnerability Assessment to complete the development of a Corrective Action Plan (Part 7.2). Second, Requirement R7 Part 7.3 was added to provide that each entity shall include an implementation timetable in its Corrective Action Plan. This timetable, which would be subject to revision under the process described in Part 7.4, shall: (i) specify implementation of non-hardware mitigation, if any, within two years of development of the Corrective Action Plan; and (ii) specify implementation of hardware mitigation, if any, within four years of development of the Corrective Action Plan.

The Variance in proposed Reliability Standard TPL-007-3 would replace Requirement R7 Part 7.3 in its entirety with Variance Requirement R7 Part D.A.7.3. The Variance would thus modify the continent-wide Requirement as follows:

R7. Each responsible entity, as determined in Requirement R1, that concludes through the benchmark GMD Vulnerability Assessment conducted in Requirement R4 that their System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1, shall develop a Corrective Action Plan (CAP) addressing how the performance requirements will be met. The CAP shall:

***

[30] *Supra* note 20.

~~**7.3.** Include a timetable, subject to revision by the responsible entity in Part 7.4, for implementing the selected actions from Part 7.1. The timetable shall:~~

~~**7.3.1.** Specify implementation of non-hardware mitigation, if any, within two years of development of the CAP; and~~

~~**7.3.2.** Specify implementation of hardware mitigation, if any, within four years of development of the CAP.~~

D.A.7.3. Include a timetable, subject to revision by the responsible entity in Part 7.4, for implementing the selected actions from Part 7.1. The timetable shall:

D.A.7.3.1. Specify implementation of non-hardware mitigation, if any, within two years of the later of the development of the CAP or receipt of regulatory approvals, if required; and

D.A.7.3.2. Specify implementation of hardware mitigation, if any, within four years of the later of the development of the CAP or receipt of regulatory approvals, if required.

The only difference between Variance Requirement R7 Part D.A.7.3 and continent-wide Requirement R7 Part 7.3 is that the Variance would require entities to specify, in their Corrective Action Plans, that mitigation actions shall be implemented by "the later of the development of the [Corrective Action Plan] or receipt of regulatory approvals, if required."

The Variance would continue to require entities to take prompt action to address any GMD vulnerabilities they identify in their systems, but it recognizes that the timing for implementing corrective actions may ultimately depend on obtaining required regulatory approvals. In such cases, it would reduce the entity's administrative burden to allow for such a contingency at the time the Corrective Action Plan is developed.

4. VAR-001-5

On October 15, 2018, FERC issued a delegated order approving revised Reliability Standard VAR-001-5 (Voltage and Reactive Control) and the retirement of currently-effective

Reliability Standard VAR-001-4.2.[31] Reliability Standard VAR-001-5 revises the Regional Variance for the Western Electricity Coordinating Council ("WECC"), which applies only to entities in the Western Interconnection.

The purpose of Reliability Standard VAR-001-5 is to ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection. The WECC Regional Variance replaces continent-wide Requirement R5, which requires each Transmission Operator to specify either a voltage or Reactive Power schedule, with Variance Requirements pertaining to voltage schedules.

III. CONCLUSION

NERC respectfully requests that the NSUARB approve the Reliability Standards as specified herein.

Respectfully submitted,

/s/ *Shamai Elstein*

Shamai Elstein
Assistant General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 28, 2019

[31] *Supra* note 15.

Exhibit A-(1): List of Reliability Standards Proposed for Approval

Reliability Standards	Effective Dates
Critical Infrastructure Protection (CIP) Standards	
CIP-005-6*	7/1/2020
CIP-010-3*	7/1/2020
CIP-013-1*	7/1/2020
Personnel Performance, Training, and Qualifications (PER) Standard	
PER-003-2*	7/1/2019
Transmission Planning (TPL) Standard	
TPL-007-3[1]	*See* Exhibit A-(4)
Voltage and Reactive (VAR) Standard	
VAR-001-5	1/1/2019

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

[1] The NERC Board of Trustees adopted proposed Reliability Standard TPL-007-3 on February 7, 2019. As discussed previously in this filing, proposed Reliability Standard TPL-007-3 supersedes TPL-007-2. As proposed Reliability Standard TPL-007-3 was modified to include a Variance for Canadian registered entities and will not be filed for FERC approval, NERC submits proposed Reliability Standard TPL-007-3 for NSUARB approval in this filing.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard CIP-005-6	
Purpose	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
Applicability	• Balancing Authorities • Distribution Provider r that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: o Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard. o Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started. • Generator Operators • Generator Owners • Interchange Coordinator or Interchange Authorities • Reliability Coordinators • Transmission Operators • Transmission Owners
Requirements	Reliability Standard CIP-005-6 includes two requirements.

Date of Petition and FERC Order	Petition filed on September 26, 2017 for approval of proposed Reliability Standard CIP-005-6 with the Federal Energy Regulatory Commission ("FERC") in Docket No. RM17-13-000. FERC approved the CIP standard on October 18, 2018.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard CIP-010-3	
Purpose	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
Applicability	• Balancing Authorities • Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: o Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard. o Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started. • Generator Operators • Generator Owners • Interchange Coordinator or Interchange Authorities • Reliability Coordinators • Transmission Operators • Transmission Owners
Requirements	Reliability Standard CIP-010-3 includes four requirements.

Date of Petition and FERC Order	Petition filed on September 26, 2017 for approval of proposed Reliability Standard CIP-010-3 with FERC in Docket No. RM17-13-000. FERC approved the CIP standard on October 18, 2018.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard CIP-013-1	
Purpose	To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.
Applicability	• Balancing Authorities • Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: o Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that: ▪ is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ▪ performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. o Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard. o Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard. • Generator Operators • Generator Owners • Reliability Coordinators • Transmission Operators • Transmission Owners
Requirements	Reliability Standard CIP-013-1 includes three requirements.
Date of Petition and FERC Order	Petition filed on September 26, 2017 for approval of proposed Reliability Standard CIP-013-1 with FERC in Docket No. RM17-13-000. FERC approved the CIP standard on October 18, 2018.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard PER-003-2	
Purpose	To ensure that System Operators performing the reliability-related tasks of the Reliability Coordinator, Balancing Authority and Transmission Operator are certified through the NERC System Operator Certification Program when filling a Realtime operating position responsible for control of the Bulk Electric System.
Applicability	• Reliability Coordinators • Transmission Operators • Balancing Authorities
Requirements	Reliability Standard PER-003-2 includes three requirements.
Date of Petition and FERC Order	Petition filed on July 23, 2018 for approval of proposed Reliability Standard PER-003-2 with FERC in Docket No. RD18-9-000. FERC approved the PER standard on November 21, 2018.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard TPL-007-3	
Purpose	Establish requirements for Transmission system planned performance during geomagnetic disturbance (GMD) events.
Applicability	• Planning Coordinator with a planning area that includes a Facility or Facilities • Transmission Planner with a planning area that includes a Facility or Facilities • Transmission Owner who owns a Facility or Facilities • Generator Owner who owns a Facility or Facilities
Requirements	Reliability Standard TPL-007-3 includes twelve requirements, four tables and seven figures.
Summary of Standard	The NERC Board of Trustees adopted proposed Reliability Standard TPL-007-3 on February 7, 2019. Proposed Reliability Standard TPL-007-3 supersedes TPL-007-2. As proposed Reliability Standard TPL-007-3 was modified to include a Variance for Canadian registered entities and will not be filed for FERC approval, NERC submits proposed Reliability Standard TPL-007-3 for NSUARB approval in this filing.

Exhibit A-(2): Informational Summary of Each Reliability Standard Proposed for Approval

Reliability Standard VAR-001-5	
Purpose	To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.
Applicability	• Transmission Planners • Generator Operators within the Western Interconnection (for the WECC Variance)
Requirements	Reliability Standard VAR-001-5 includes six requirements.
Date of Petition and FERC Order	Petition filed on September 6, 2018 for approval of proposed Reliability Standard VAR-001-5 with FERC in Docket No. RD18-8-000. FERC approved the VAR standard on October 15, 2018.

Exhibit A-(3): Reliability Standards Proposed for Approval

CIP-005-6

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-6:

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 identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-005 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 Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"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 "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high 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.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **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.
- **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.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points 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 processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. 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 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	

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. Furthermore,

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'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:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: CIP-005-6 — Cyber Security — Electronic Security Perimeter(s)

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
CIP-005-6	All	07/01/2020		

Printed On: January 07, 2019, 12:06 PM

CIP-010-3

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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 identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-010 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 applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **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 process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

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

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

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:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the

SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
CIP-010-3	All	07/01/2020		

Printed On: January 07, 2019, 12:07 PM

CIP-013-1

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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 (ESPs).

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 identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" 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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

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

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

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

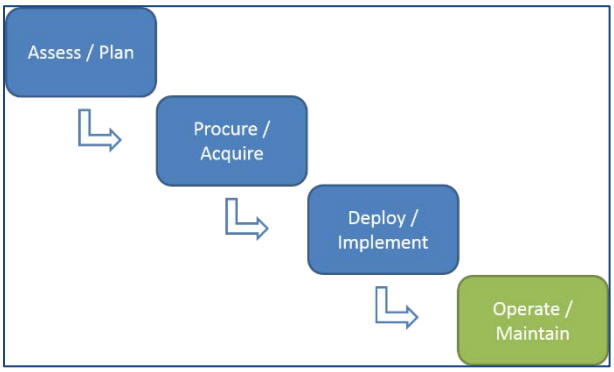
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the

awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: CIP-013-1 — Cyber Security - Supply Chain Risk Management

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
CIP-013-1	All	07/01/2020		

Printed On: January 07, 2019, 12:07 PM

PER-003-2

A. Introduction

1. **Title:** **Operating Personnel Credentials**

2. **Number:** **PER-003-2**

3. **Purpose:** To ensure that System Operators performing the reliability-related tasks of the Reliability Coordinator, Balancing Authority and Transmission Operator are certified through the NERC System Operator Certification Program when filling a Real-time operating position responsible for control of the Bulk Electric System.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Reliability Coordinator

   4.1.2. Transmission Operator

   4.1.3. Balancing Authority

5. **Effective Date:** See Implementation Plan for standard PER-003-2.

B. Requirements and Measures

R1. Each Reliability Coordinator shall staff its Real-time operating positions performing Reliability Coordinator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining a valid NERC Reliability Operator certificate [(1)(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*

1.1. Areas of Competency

1.1.1. Resource and demand balancing

1.1.2. Transmission operations

1.1.3. Emergency preparedness and operations

1.1.4. System operations

1.1.5. Protection and control

1.1.6. Voltage and reactive

1.1.7. Interchange scheduling and coordination

1.1.8. Interconnection reliability operations and coordination

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M1. Each Reliability Coordinator shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

M1.1 A list of Real-time operating positions.

M1.2 A list of System Operators assigned to its Real-time operating positions.

M1.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

M1.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

R2. Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates [(1)][(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*:

2.1. Areas of Competency

2.1.1. Transmission operations

2.1.2. Emergency preparedness and operations

2.1.3. System operations

2.1.4. Protection and control

2.1.5. Voltage and reactive

2.2. Certificates

- Reliability Operator
- Balancing, Interchange and Transmission Operator
- Transmission Operator

M2. Each Transmission Operator shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M2.1 A list of Real-time operating positions.

M2.2 A list of System Operators assigned to its Real-time operating positions.

M2.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

M2.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

R3. Each Balancing Authority shall staff its Real-time operating positions performing Balancing Authority reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates [(1)(2)]: *[Risk Factor: High][Time Horizon: Real-time Operations]*:

3.1. Areas of Competency

3.1.1. Resources and demand balancing

3.1.2. Emergency preparedness and operations

3.1.3. System operations

3.1.4. Interchange scheduling and coordination

3.2. Certificates

- Reliability Operator
- Balancing, Interchange and Transmission Operator
- Balancing and Interchange Operator

M3. Each Balancing Authority shall have the following evidence to show that it staffed its Real-time operating positions performing reliability-related tasks with System Operators who have demonstrated the applicable minimum competency by obtaining and maintaining the appropriate, valid NERC certificate:

M3.1 A list of Real-time operating positions.

M3.2 A list of System Operators assigned to its Real-time operating positions.

M3.3 A copy of each of its System Operator's NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

---

[1] Non-NERC certified personnel performing any reliability-related task of a real-time operating position must be under the direct supervision of a NERC Certified System Operator stationed at that operating position; the NERC Certified System Operator at that operating position has ultimate responsibility for the performance of the reliability-related tasks.

[2] The NERC certificates referenced in this standard pertain to those certificates identified in the NERC System Operator Certification Program Manual.

M3.4 Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Reliability Coordinator, Transmission Operator and Balancing Authority shall keep data or evidence for three years or since its last compliance audit, whichever time frame is the greatest.

1.3. Compliance Monitoring and Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Reliability Coordinator failed to staff each Real-time operating position performing Reliability Coordinator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R1.
R2.	N/A	N/A	N/A	The Transmission Operator failed to staff each Real-time operating position performing Transmission Operator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R2, Part 2.2.
R3.	N/A	N/A	N/A	The Balancing Authority failed to staff each Real-time operating position performing Balancing Authority reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R3, Part 3.2.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	February 17, 2011	Complete revision under Project 2007-04	Revision
1	February 17, 2011	Adopted by Board of Trustees	
1	September 15, 2011	FERC Order issued by FERC approving PER-003-1 (effective date of the Order is September 15, 2011)	
2	May 10, 2018	Added footnote to requirements	Revision
2	May 10, 2018	Adopted by Board of Trustees	Revision

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: PER-003-2 — Operating Personnel Credentials

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
PER-003-2	All			

This standard has not yet been approved by the applicable regulatory authority.

Printed On: January 09, 2019, 03:59 PM

TPL-007-3

A. Introduction

1. **Title:** Transmission System Planned Performance for Geomagnetic Disturbance Events

2. **Number:** TPL-007-3

3. **Purpose:** Establish requirements for Transmission system planned performance during geomagnetic disturbance (GMD) events.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1. Planning Coordinator with a planning area that includes a Facility or Facilities specified in 4.2;

   4.1.2. Transmission Planner with a planning area that includes a Facility or Facilities specified in 4.2;

   4.1.3. Transmission Owner who owns a Facility or Facilities specified in 4.2; and

   4.1.4. Generator Owner who owns a Facility or Facilities specified in 4.2.

   4.2. Facilities:

   4.2.1. Facilities that include power transformer(s) with a high side, wye-grounded winding with terminal voltage greater than 200 kV.

5. **Effective Date:** See Implementation Plan for TPL-007-3.

Background: During a GMD event, geomagnetically-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Misoperation(s), the combination of which may result in voltage collapse and blackout.

The only difference between TPL-007-3 and TPL-007-2 is that TPL-007-3 adds a Canadian Variance to address regulatory practices/processes within Canadian jurisdictions and to allow the use of Canadian-specific data and research to define and implement alternative GMD event(s) that achieve at least an equivalent reliability objective of that in TPL-007-2.

B. Requirements and Measures

R1. Each Planning Coordinator, in conjunction with its Transmission Planner(s), shall identify the individual and joint responsibilities of the Planning Coordinator and Transmission Planner(s) in the Planning Coordinator's planning area for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data as specified in this standard. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M1. Each Planning Coordinator, in conjunction with its Transmission Planners, shall provide documentation on roles and responsibilities, such as meeting minutes, agreements, copies of procedures or protocols in effect between entities or between departments of a vertically integrated system, or email correspondence that identifies an agreement has been reached on individual and joint responsibilities for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data in accordance with Requirement R1.

R2. Each responsible entity, as determined in Requirement R1, shall maintain System models and GIC System models of the responsible entity's planning area for performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M2. Each responsible entity, as determined in Requirement R1, shall have evidence in either electronic or hard copy format that it is maintaining System models and GIC System models of the responsible entity's planning area for performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments.

R3. Each responsible entity, as determined in Requirement R1, shall have criteria for acceptable System steady state voltage performance for its System during the GMD events described in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each responsible entity, as determined in Requirement R1, shall have evidence, such as electronic or hard copies of the criteria for acceptable System steady state voltage performance for its System in accordance with Requirement R3.

Benchmark GMD Vulnerability Assessment(s)

R4. Each responsible entity, as determined in Requirement R1, shall complete a benchmark GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon at least once every 60 calendar months. This benchmark GMD Vulnerability Assessment shall use a study or studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

4.1. The study or studies shall include the following conditions:

4.1.1. System On-Peak Load for at least one year within the Near-Term Transmission Planning Horizon; and

4.1.2. System Off-Peak Load for at least one year within the Near-Term Transmission Planning Horizon.

4.2. The study or studies shall be conducted based on the benchmark GMD event described in Attachment 1 to determine whether the System meets the performance requirements for the steady state planning benchmark GMD event contained in Table 1.

4.3. The benchmark GMD Vulnerability Assessment shall be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, and adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the benchmark GMD Vulnerability Assessment, whichever is later.

4.3.1. If a recipient of the benchmark GMD Vulnerability Assessment provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M4. Each responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its benchmark GMD Vulnerability Assessment meeting all of the requirements in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its benchmark GMD Vulnerability Assessment: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, and adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the benchmark GMD Vulnerability Assessment, whichever is later, as specified in Requirement R4. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its benchmark GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R4.

R5. Each responsible entity, as determined in Requirement R1, shall provide GIC flow information to be used for the benchmark thermal impact assessment of transformers specified in Requirement R6 to each Transmission Owner and Generator Owner that owns an applicable Bulk Electric System (BES) power transformer in the planning area. The GIC flow information shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

5.1. The maximum effective GIC value for the worst case geoelectric field orientation for the benchmark GMD event described in Attachment 1. This value shall be provided to the Transmission Owner or Generator Owner that owns each applicable BES power transformer in the planning area.

5.2. The effective GIC time series, GIC(t), calculated using the benchmark GMD event described in Attachment 1 in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area. GIC(t) shall be provided within 90 calendar days of receipt of the written request and after determination of the maximum effective GIC value in Part 5.1.

M5. Each responsible entity, as determined in Requirement R1, shall provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided the maximum effective GIC values to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area as specified in Requirement R5, Part 5.1. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided GIC(t) in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area.

R6. Each Transmission Owner and Generator Owner shall conduct a benchmark thermal impact assessment for its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A per phase or greater. The benchmark thermal impact assessment shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

6.1. Be based on the effective GIC flow information provided in Requirement R5;

6.2. Document assumptions used in the analysis;

6.3. Describe suggested actions and supporting analysis to mitigate the impact of GICs, if any; and

6.4. Be performed and provided to the responsible entities, as determined in Requirement R1, within 24 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1.

M6. Each Transmission Owner and Generator Owner shall have evidence such as electronic or hard copies of its benchmark thermal impact assessment for all of its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A per phase or greater, and shall have evidence such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided its thermal impact assessment to the responsible entities as specified in Requirement R6.

R7. Each responsible entity, as determined in Requirement R1, that concludes through the benchmark GMD Vulnerability Assessment conducted in Requirement R4 that their System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1, shall develop a Corrective

Action Plan (CAP) addressing how the performance requirements will be met. The CAP shall: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

7.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:

- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
- Installation, modification, or removal of Protection Systems or Remedial Action Schemes.
- Use of Operating Procedures, specifying how long they will be needed as part of the CAP.
- Use of Demand-Side Management, new technologies, or other initiatives.

7.2. Be developed within one year of completion of the benchmark GMD Vulnerability Assessment.

7.3. Include a timetable, subject to revision by the responsible entity in Part 7.4, for implementing the selected actions from Part 7.1. The timetable shall:

7.3.1. Specify implementation of non-hardware mitigation, if any, within two years of development of the CAP; and

7.3.2. Specify implementation of hardware mitigation, if any, within four years of development of the CAP.

7.4. Be revised if situations beyond the control of the responsible entity determined in Requirement R1 prevent implementation of the CAP within the timetable for implementation provided in Part 7.3. The revised CAP shall document the following, and be updated at least once every 12 calendar months until implemented:

7.4.1. Circumstances causing the delay for fully or partially implementing the selected actions in Part 7.1;

7.4.2. Description of the original CAP, and any previous changes to the CAP, with the associated timetable(s) for implementing the selected actions in Part 7.1; and

7.4.3. Revisions to the selected actions in Part 7.1, if any, including utilization of Operating Procedures if applicable, and the updated timetable for implementing the selected actions.

7.5. Be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later.

7.5.1. If a recipient of the CAP provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M7. Each responsible entity, as determined in Requirement R1, that concludes, through the benchmark GMD Vulnerability Assessment conducted in Requirement R4, that the responsible entity's System does not meet the performance requirements for the steady state planning benchmark GMD event contained in Table 1 shall have evidence such as dated electronic or hard copies of its CAP including timetable for implementing selected actions, as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records or postal receipts showing recipient and date, that it has revised its CAP if situations beyond the responsible entity's control prevent implementation of the CAP within the timetable specified. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its CAP or relevant information, if any, (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinator(s), adjacent Transmission Planner(s), and functional entities referenced in the CAP within 90 calendar days of development or revision, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of development or revision, whichever is later as specified in Requirement R7. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its CAP within 90 calendar days of receipt of those comments, in accordance with Requirement R7.

Supplemental GMD Vulnerability Assessment(s)

R8. Each responsible entity, as determined in Requirement R1, shall complete a supplemental GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon at least once every 60 calendar months. This supplemental GMD Vulnerability Assessment shall use a study or studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

8.1. The study or studies shall include the following conditions:

8.1.1. System On-Peak Load for at least one year within the Near-Term Transmission Planning Horizon; and

8.1.2. System Off-Peak Load for at least one year within the Near-Term Transmission Planning Horizon.

8.2. The study or studies shall be conducted based on the supplemental GMD event described in Attachment 1 to determine whether the System meets the performance requirements for the steady state planning supplemental GMD event contained in Table 1.

8.3. If the analysis concludes there is Cascading caused by the supplemental GMD event described in Attachment 1, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences and adverse impacts of the event(s) shall be conducted.

8.4. The supplemental GMD Vulnerability Assessment shall be provided: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the supplemental GMD Vulnerability Assessment, whichever is later.

8.4.1. If a recipient of the supplemental GMD Vulnerability Assessment provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M8. Each responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its supplemental GMD Vulnerability Assessment meeting all of the requirements in Requirement R8. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has distributed its supplemental GMD Vulnerability: (i) to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners within 90 calendar days of completion, and (ii) to any functional entity that submits a written request and has a reliability-related need within 90 calendar days of receipt of such request or within 90 calendar days of completion of the supplemental GMD Vulnerability Assessment, whichever is later, as specified in Requirement R8. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date, that it has provided a documented response to comments received on its supplemental GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R8.

R9. Each responsible entity, as determined in Requirement R1, shall provide GIC flow information to be used for the supplemental thermal impact assessment of transformers specified in Requirement R10 to each Transmission Owner and Generator Owner that owns an applicable Bulk Electric System (BES) power transformer in the planning area. The GIC flow information shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

9.1. The maximum effective GIC value for the worst case geoelectric field orientation for the supplemental GMD event described in Attachment 1. This value shall be provided to the Transmission Owner or Generator Owner that owns each applicable BES power transformer in the planning area.

9.2. The effective GIC time series, GIC(t), calculated using the supplemental GMD event described in Attachment 1 in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area. GIC(t) shall be provided within 90 calendar days of receipt of the written request and after determination of the maximum effective GIC value in Part 9.1.

M9. Each responsible entity, as determined in Requirement R1, shall provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided the maximum effective GIC values to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area as specified in Requirement R9, Part 9.1. Each responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided GIC(t) in response to a written request from the Transmission Owner or Generator Owner that owns an applicable BES power transformer in the planning area.

R10. Each Transmission Owner and Generator Owner shall conduct a supplemental thermal impact assessment for its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A per phase or greater. The supplemental thermal impact assessment shall: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

10.1. Be based on the effective GIC flow information provided in Requirement R9;

10.2. Document assumptions used in the analysis;

10.3. Describe suggested actions and supporting analysis to mitigate the impact of GICs, if any; and

10.4. Be performed and provided to the responsible entities, as determined in Requirement R1, within 24 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1.

M10. Each Transmission Owner and Generator Owner shall have evidence such as electronic or hard copies of its supplemental thermal impact assessment for all of its solely and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A per phase or greater, and shall have evidence such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date, that it has provided its supplemental thermal impact assessment to the responsible entities as specified in Requirement R10.

GMD Measurement Data Processes

R11. Each responsible entity, as determined in Requirement R1, shall implement a process to obtain GIC monitor data from at least one GIC monitor located in the Planning Coordinator's planning area or other part of the system included in the Planning Coordinator's GIC System model. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M11. Each responsible entity, as determined in Requirement R1, shall have evidence such as electronic or hard copies of its GIC monitor location(s) and documentation of its process to obtain GIC monitor data in accordance with Requirement R11.

R12. Each responsible entity, as determined in Requirement R1, shall implement a process to obtain geomagnetic field data for its Planning Coordinator's planning area. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M12. Each responsible entity, as determined in Requirement R1, shall have evidence such as electronic or hard copies of its process to obtain geomagnetic field data for its Planning Coordinator's planning area in accordance with Requirement R12.

C. Compliance

1. Compliance Monitoring Process

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

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

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

- For Requirements R1, R2, R3, R5, R6, R9, and R10, each responsible entity shall retain documentation as evidence for five years.
- For Requirements R4 and R8, each responsible entity shall retain documentation of the current GMD Vulnerability Assessment and the preceding GMD Vulnerability Assessment.

- For Requirement R7, each responsible entity shall retain documentation as evidence for five years or until all actions in the Corrective Action Plan are completed, whichever is later.
- For Requirements R11 and R12, each responsible entity shall retain documentation as evidence for three years.

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.

Table 1: Steady State Planning GMD Event

Steady State:

a. Voltage collapse, Cascading and uncontrolled islanding shall not occur.
b. Generation loss is acceptable as a consequence of the steady state planning GMD events.
c. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

Category	Initial Condition	Event	Interruption of Firm Transmission Service Allowed	Load Loss Allowed
Benchmark GMD Event - GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation or Misoperation due to harmonics during the GMD event	Yes[3]	Yes[3]
Supplemental GMD Event - GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation or Misoperation due to harmonics during the GMD event	Yes	Yes

Table 1: Steady State Performance Footnotes

1. The System condition for GMD planning may include adjustments to posture the System that are executable in response to space weather information.
2. The GMD conditions for the benchmark and supplemental planning events are described in Attachment 1.
3. Load loss as a result of manual or automatic Load shedding (e.g., UVLS) and/or curtailment of Firm Transmission Service may be used to meet BES performance requirements during studied GMD conditions. The likelihood and magnitude of Load loss or curtailment of Firm Transmission Service should be minimized.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Planning Coordinator, in conjunction with its Transmission Planner(s), failed to determine and identify individual or joint responsibilities of the Planning Coordinator and Transmission Planner(s) in the Planning Coordinator's planning area for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data as specified in this standard.
R2.	N/A	N/A	The responsible entity did not maintain either System models or GIC System models of the responsible entity's planning area for performing the studies	The responsible entity did not maintain both System models and GIC System models of the responsible entity's planning area for performing the studies

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			needed to complete benchmark and supplemental GMD Vulnerability Assessments.	needed to complete benchmark and supplemental GMD Vulnerability Assessments.
R3.	N/A	N/A	N/A	The responsible entity did not have criteria for acceptable System steady state voltage performance for its System during the GMD events described in Attachment 1 as required.
R4.	The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 60 calendar months and less than or equal to 64 calendar months since the last benchmark GMD Vulnerability Assessment.	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy one of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 64 calendar months and less than or equal to 68 calendar months since the	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy two of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 68 calendar months and less than or equal to 72 calendar months since the	The responsible entity's completed benchmark GMD Vulnerability Assessment failed to satisfy three of the elements listed in Requirement R4, Parts 4.1 through 4.3; OR The responsible entity completed a benchmark GMD Vulnerability Assessment, but it was more than 72 calendar months since the last benchmark

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		last benchmark GMD Vulnerability Assessment.	last benchmark GMD Vulnerability Assessment.	GMD Vulnerability Assessment; OR The responsible entity does not have a completed benchmark GMD Vulnerability Assessment.
R5.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 90 calendar days and less than or equal to 100 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 100 calendar days and less than or equal to 110 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 110 calendar days after receipt of a written request.	The responsible entity did not provide the maximum effective GIC value to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area; OR The responsible entity did not provide the effective GIC time series, GIC(t), upon written request.
R6.	The responsible entity failed to conduct a benchmark thermal impact assessment for 5% or less or one of its solely owned and jointly owned applicable BES power	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 5% up to (and including) 10% or two of its solely owned and jointly	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 10% up to (and including) 15% or three of its solely owned and	The responsible entity failed to conduct a benchmark thermal impact assessment for more than 15% or more than three of its solely owned and jointly owned

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 24 calendar months and less than or equal to 26 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1.	owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 26 calendar months and less than or equal to 28 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include one of the	jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 28 calendar months and less than or equal to 30 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include two of the	applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase; OR The responsible entity conducted a benchmark thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R5, Part 5.1, is 75 A or greater per phase but did so more than 30 calendar months of receiving GIC flow information specified in Requirement R5, Part 5.1; OR The responsible entity failed to include three of the required elements as listed

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		required elements as listed in Requirement R6, Parts 6.1 through 6.3.	required elements as listed in Requirement R6, Parts 6.1 through 6.3.	in Requirement R6, Parts 6.1 through 6.3.
R7.	The responsible entity's Corrective Action Plan failed to comply with one of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with two of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with three of the elements in Requirement R7, Parts 7.1 through 7.5.	The responsible entity's Corrective Action Plan failed to comply with four or more of the elements in Requirement R7, Parts 7.1 through 7.5; OR The responsible entity did not have a Corrective Action Plan as required by Requirement R7.
R8.	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy one of elements listed in Requirement R8, Parts 8.1 through 8.4; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy two of elements listed in Requirement R8, Parts 8.1 through 8.4; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy three of the elements listed in Requirement R8, Parts 8.1 through 8.4; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more	The responsible entity's completed supplemental GMD Vulnerability Assessment failed to satisfy four of the elements listed in Requirement R8, Parts 8.1 through 8.4; OR The responsible entity completed a supplemental GMD Vulnerability Assessment, but it was more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	than 60 calendar months and less than or equal to 64 calendar months since the last supplemental GMD Vulnerability Assessment.	than 64 calendar months and less than or equal to 68 calendar months since the last supplemental GMD Vulnerability Assessment.	than 68 calendar months and less than or equal to 72 calendar months since the last supplemental GMD Vulnerability Assessment.	than 72 calendar months since the last supplemental GMD Vulnerability Assessment; OR The responsible entity does not have a completed supplemental GMD Vulnerability Assessment.
R9.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 90 calendar days and less than or equal to 100 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 100 calendar days and less than or equal to 110 calendar days after receipt of a written request.	The responsible entity provided the effective GIC time series, GIC(t), in response to written request, but did so more than 110 calendar days after receipt of a written request.	The responsible entity did not provide the maximum effective GIC value to the Transmission Owner and Generator Owner that owns each applicable BES power transformer in the planning area; OR The responsible entity did not provide the effective GIC time series, GIC(t), upon written request.
R10.	The responsible entity failed to conduct a supplemental thermal impact assessment for 5% or less or one of its	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 5% up to (and	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 10% up to	The responsible entity failed to conduct a supplemental thermal impact assessment for more than 15% or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 24 calendar months and less than or equal to 26 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1.	including) 10% or two of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 26 calendar months and less than or equal to 28 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1 OR	(and including) 15% or three of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 28 calendar months and less than or equal to 30 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1; OR	than three of its solely owned and jointly owned applicable BES power transformers (whichever is greater) where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase; OR The responsible entity conducted a supplemental thermal impact assessment for its solely owned and jointly owned applicable BES power transformers where the maximum effective GIC value provided in Requirement R9, Part 9.1, is 85 A or greater per phase but did so more than 30 calendar months of receiving GIC flow information specified in Requirement R9, Part 9.1; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The responsible entity failed to include one of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.	The responsible entity failed to include two of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.	The responsible entity failed to include three of the required elements as listed in Requirement R10, Parts 10.1 through 10.3.
R11.	N/A	N/A	N/A	The responsible entity did not implement a process to obtain GIC monitor data from at least one GIC monitor located in the Planning Coordinator's planning area or other part of the system included in the Planning Coordinator's GIC System Model.
R12.	N/A	N/A	N/A	The responsible entity did not implement a process to obtain geomagnetic field data for its Planning Coordinator's planning area.

D. Regional Variances

D.A. Regional Variance for Canadian Jurisdictions

This Variance shall be applicable in those Canadian jurisdictions where the Variance has been approved for use by the applicable governmental authority or has otherwise become effective in the jurisdiction.

All references to "Attachment 1" in the standard are replaced with "Attachment 1 or Attachment 1-CAN."

In addition, this Variance replaces Requirement R7, Part 7.3 with the following:

D.A.7.3. Include a timetable, subject to revision by the responsible entity in Part 7.4, for implementing the selected actions from Part 7.1. The timetable shall:

D.A.7.3.1. Specify implementation of non-hardware mitigation, if any, within two years of the later of the development of the CAP or receipt of regulatory approvals, if required; and

D.A.7.3.2. Specify implementation of hardware mitigation, if any, within four years of the later of the development of the CAP or receipt of regulatory approvals, if required.

E. Associated Documents

Attachment 1

Attachment 1-CAN

Version History

Version	Date	Action	Change Tracking
1	December 17, 2014	Adopted by the NERC Board of Trustees	New
2	November 9, 2017	Adopted by the NERC Board of Trustees	Revised to respond to directives in FERC Order No. 830.
2	November 25, 2018	FERC Order issued approving TPL-007-2. Docket No. RM18-8-000	
3	February 7, 2019	Adopted by the NERC Board of Trustees	Canadian Variance

Attachment 1

Calculating Geoelectric Fields for the Benchmark and Supplemental GMD Events

The benchmark GMD event[1] defines the geoelectric field values used to compute GIC flows that are needed to conduct a benchmark GMD Vulnerability Assessment. It is composed of the following elements: (1) a reference peak geoelectric field amplitude of 8 V/km derived from statistical analysis of historical magnetometer data; (2) scaling factors to account for local geomagnetic latitude; (3) scaling factors to account for local earth conductivity; and (4) a reference geomagnetic field time series or waveform to facilitate time-domain analysis of GMD impact on equipment.

The supplemental GMD event is composed of similar elements as described above, except (1) the reference peak geoelectric field amplitude is 12 V/km over a localized area; and (2) the geomagnetic field time series or waveform includes a local enhancement in the waveform.[2]

The regional geoelectric field peak amplitude used in GMD Vulnerability Assessment, E_{peak}, can be obtained from the reference geoelectric field value of 8 V/km for the benchmark GMD event (1) or 12 V/km for the supplemental GMD event (2) using the following relationships:

$$E_{peak} = 8 \times \alpha \times \beta_{\,b}\ (V/km) \quad (1)$$

$$E_{peak} = 12 \times \alpha \times \beta_{\,s}\ (V/km) \quad (2)$$

where, α is the scaling factor to account for local geomagnetic latitude, and β is a scaling factor to account for the local earth conductivity structure. Subscripts *b* and *s* for the β scaling factor denote association with the benchmark or supplemental GMD events, respectively.

Scaling the Geomagnetic Field

The benchmark and supplemental GMD events are defined for geomagnetic latitude of 60° and must be scaled to account for regional differences based on geomagnetic latitude. Table 2 provides a scaling factor correlating peak geoelectric field to geomagnetic latitude. Alternatively, the scaling factor α is computed with the empirical expression:

$$\alpha = 0.001 \times e^{(0.115 \times L)} \quad (3)$$

where, L is the geomagnetic latitude in degrees and $0.1 \leq \alpha \leq 1$.

[1] The Benchmark Geomagnetic Disturbance Event Description, May 2016 is available on the Related Information webpage for TPL-007-1: http://www.nerc.com/pa/Stand/TPL0071RD/Benchmark_clean_May12_complete.pdf.

[2] The extent of local enhancements is on the order of 100 km in North-South (latitude) direction but longer in East-West (longitude) direction. The local enhancement in the geomagnetic field occurs over the time period of 2-5 minutes. Additional information is available in the Supplemental Geomagnetic Disturbance Event Description, October 2017 white paper on the Project 2013-03 Geomagnetic Disturbance Mitigation project webpage: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

For large planning areas that cover more than one scaling factor from Table 2, the GMD Vulnerability Assessment should be based on a peak geoelectric field that is:

- calculated by using the most conservative (largest) value for α; or
- calculated assuming a non-uniform or piecewise uniform geomagnetic field.

Table 2: Geomagnetic Field Scaling Factors for the Benchmark and Supplemental GMD Events

Geomagnetic Latitude (Degrees)	Scaling Factor1 (α)
≤ 40	0.10
45	0.2
50	0.3
54	0.5
56	0.6
57	0.7
58	0.8
59	0.9
≥ 60	1.0

Scaling the Geoelectric Field

The benchmark GMD event is defined for the reference Quebec earth model described in Table 4. The peak geoelectric field, E_{peak}, used in a GMD Vulnerability Assessment may be obtained by either:

- Calculating the geoelectric field for the ground conductivity in the planning area and the reference geomagnetic field time series scaled according to geomagnetic latitude, using a procedure such as the plane wave method described in the NERC GMD Task Force GIC Application Guide;[3] or
- Using the earth conductivity scaling factor β from Table 3 that correlates to the ground conductivity map in Figure 1 or Figure 2. Along with the scaling factor α from equation (3) or Table 2, β is applied to the reference geoelectric field using equation (1 or 2, as applicable) to obtain the regional geoelectric field peak amplitude E_{peak} to be used in GMD Vulnerability Assessments. When a ground conductivity model is not available, the planning entity should use the largest β factor of adjacent physiographic regions or a technically justified value.

[3] Available at the NERC GMD Task Force project webpage: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx.

The earth models used to calculate Table 3 for the United States were obtained from publicly available information published on the U. S. Geological Survey website.[4] The models used to calculate Table 3 for Canada were obtained from Natural Resources Canada (NRCan) and reflect the average structure for large regions. A planner can also use specific earth model(s) with documented justification and the reference geomagnetic field time series to calculate the β factor(s) as follows:

$$\beta_b = E/8 \text{ for the benchmark GMD event} \quad (4)$$

$$\beta_s = E/12 \text{ for the supplemental GMD} \quad (5)$$

where, *E* is the absolute value of peak geoelectric in V/km obtained from the technically justified earth model and the reference geomagnetic field time series.

For large planning areas that span more than one β scaling factor, the most conservative (largest) value for β may be used in determining the peak geoelectric field to obtain conservative results. Alternatively, a planner could perform analysis using a non-uniform or piecewise uniform geoelectric field.

Applying the Localized Peak Geoelectric Field in the Supplemental GMD Event

The peak geoelectric field of the supplemental GMD event occurs in a localized area.[5] Planners have flexibility to determine how to apply the localized peak geoelectric field over the planning area in performing GIC calculations. Examples of approaches are:

- Apply the peak geoelectric field (12 V/km scaled to the planning area) over the entire planning area;
- Apply a spatially limited (12 V/km scaled to the planning area) peak geoelectric field (e.g., 100 km in North-South latitude direction and 500 km in East-West longitude direction) over a portion(s) of the system, and apply the benchmark GMD event over the rest of the system; or
- Other methods to adjust the benchmark GMD event analysis to account for the localized geoelectric field enhancement of the supplemental GMD event.

[4] Available at http://geomag.usgs.gov/conductivity/.
[5] See the Supplemental Geomagnetic Disturbance Description white paper located on the Project 2013-03 Geomagnetic Disturbance Mitigation project webpage: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

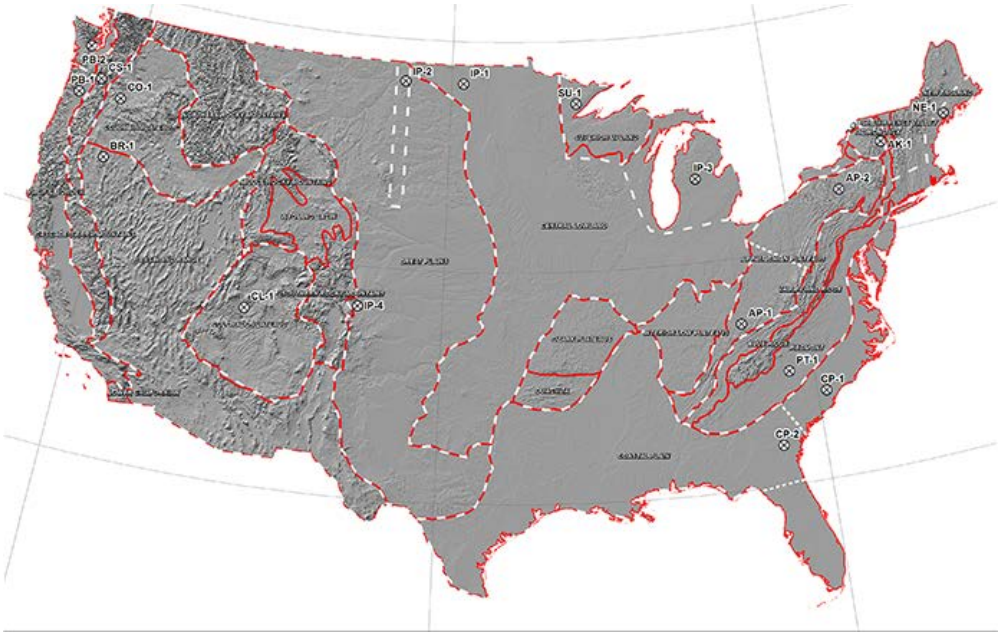


Figure 1: Physiographic Regions of the Continental United States[6]

Figure 2: Physiographic Regions of Canada

[6] Additional map detail is available at the U.S. Geological Survey: http://geomag.usgs.gov/.

Table 3: Geoelectric Field Scaling Factors		
Earth model	**Scaling Factor Benchmark Event (β_b)**	**Scaling Factor Supplemental Event (β_s)**
AK1A	0.56	0.51
AK1B	0.56	0.51
AP1	0.33	0.30
AP2	0.82	0.78
BR1	0.22	0.22
CL1	0.76	0.73
CO1	0.27	0.25
CP1	0.81	0.77
CP2	0.95	0.86
FL1	0.76	0.73
CS1	0.41	0.37
IP1	0.94	0.90
IP2	0.28	0.25
IP3	0.93	0.90
IP4	0.41	0.35
NE1	0.81	0.77
PB1	0.62	0.55
PB2	0.46	0.39
PT1	1.17	1.19
SL1	0.53	0.49
SU1	0.93	0.90
BOU	0.28	0.24
FBK	0.56	0.56
PRU	0.21	0.22
BC	0.67	0.62
PRAIRIES	0.96	0.88
SHIELD	1.0	1.0
ATLANTIC	0.79	0.76

Rationale: Scaling factors in Table 3 are dependent upon the frequency content of the reference storm. Consequently, the benchmark GMD event and the supplemental GMD event may produce different scaling factors for a given earth model.

The scaling factor associated with the benchmark GMD event for the Florida earth model (FL1) has been updated based on the earth model published on the USGS public website.

Table 4: Reference Earth Model (Quebec)

Layer Thickness (km)	Resistivity (Ω-m)
15	20,000
10	200
125	1,000
200	100
∞	3

Reference Geomagnetic Field Time Series or Waveform for the Benchmark GMD Event[7]

The geomagnetic field measurement record of the March 13-14 1989 GMD event, measured at the NRCan Ottawa geomagnetic observatory, is the basis for the reference geomagnetic field waveform to be used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitudes of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see Figure 3) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 8 V/km (see Figures 4 and 5). The sampling rate for the geomagnetic field waveform is 10 seconds.[8] To use this geoelectric field time series when a different earth model is applicable, it should be scaled with the appropriate benchmark conductivity scaling factor β_b.

[7] Refer to the Benchmark Geomagnetic Disturbance Event Description white paper for details on the determination of the reference geomagnetic field waveform: http://www.nerc.com/pa/stand/Pages/TPL0071RI.aspx.

[8] The data file of the benchmark geomagnetic field waveform is available on the Related Information webpage for TPL-007-1: http://www.nerc.com/pa/stand/Pages/TPL0071RI.aspx.

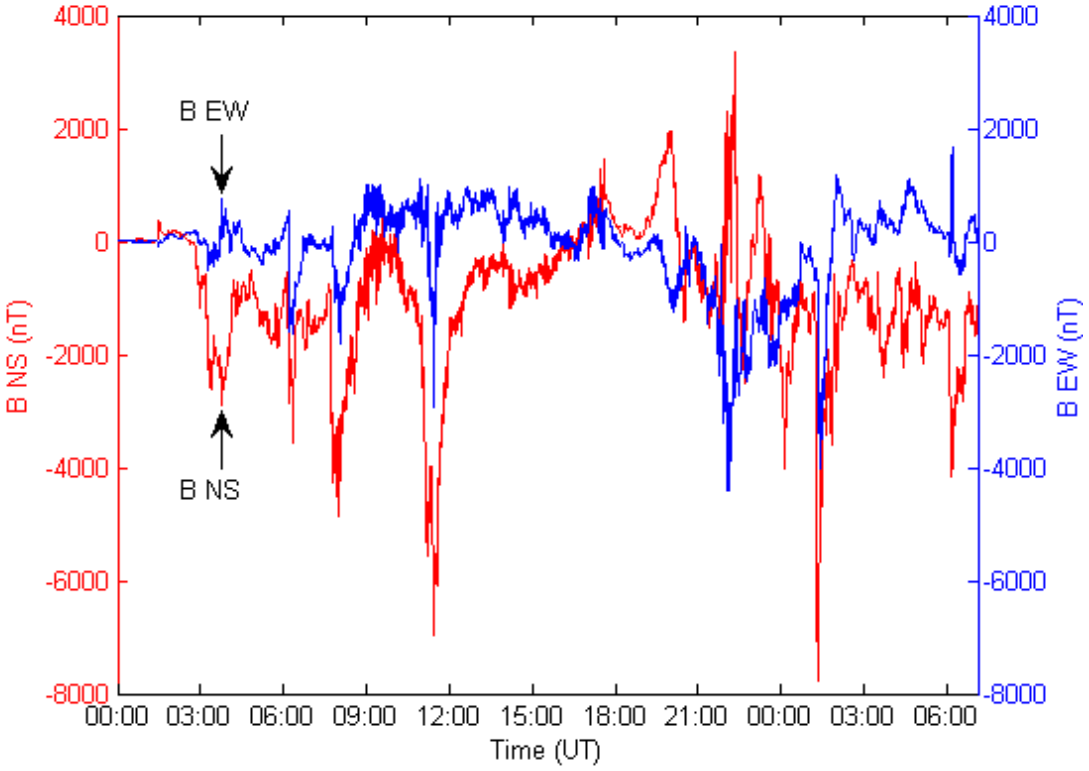


Figure 3: Benchmark Geomagnetic Field Waveform
Red B_n (Northward), Blue B_e (Eastward)

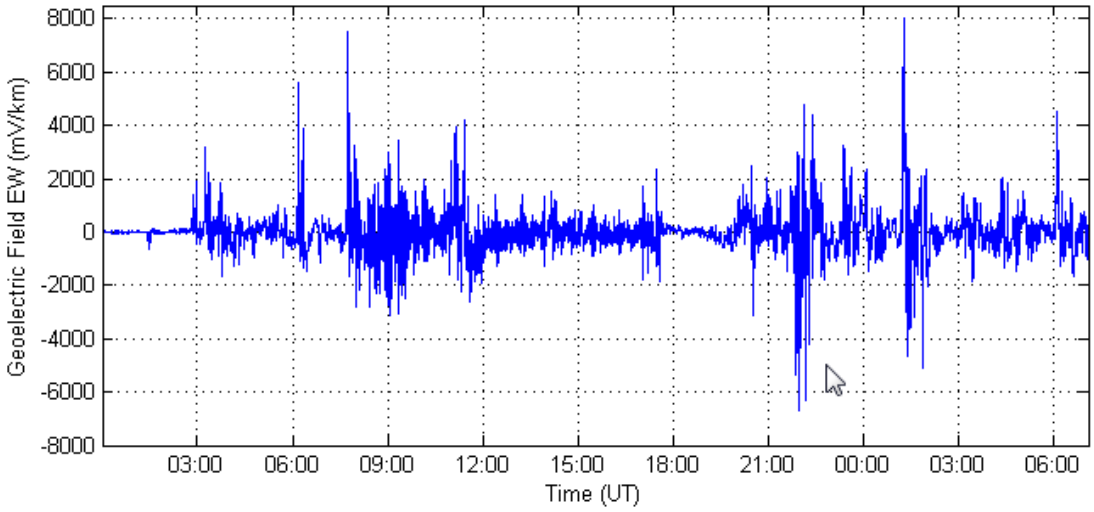


Figure 4: Benchmark Geoelectric Field Waveform
E_E (Eastward)

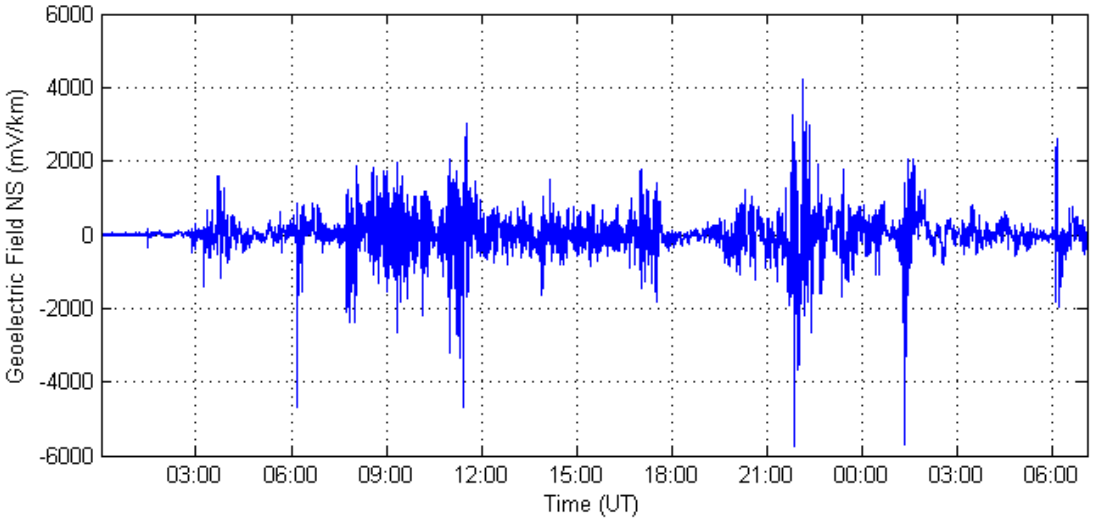


Figure 5: Benchmark Geoelectric Field Waveform
E_N (Northward)

Reference Geomagnetic Field Time Series or Waveform for the Supplemental GMD Event[9]

The geomagnetic field measurement record of the March 13-14, 1989 GMD event, measured at the NRCan Ottawa geomagnetic observatory, is the basis for the reference geomagnetic field waveform to be used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment for the supplemental GMD event. The supplemental GMD event waveform differs from the benchmark GMD event waveform in that the supplemental GMD event waveform has a local enhancement.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitudes of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see Figure 6) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 12 V/km (see Figure7). The sampling rate for the geomagnetic field waveform is 10 seconds.[10] To use this geoelectric field time series when a different earth model is applicable, it should be scaled with the appropriate supplemental conductivity scaling factor β_s.

[9] Refer to the Supplemental Geomagnetic Disturbance Event Description white paper for details on the determination of the reference geomagnetic field waveform: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

[10] The data file of the benchmark geomagnetic field waveform is available on the NERC GMD Task Force project webpage: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx.

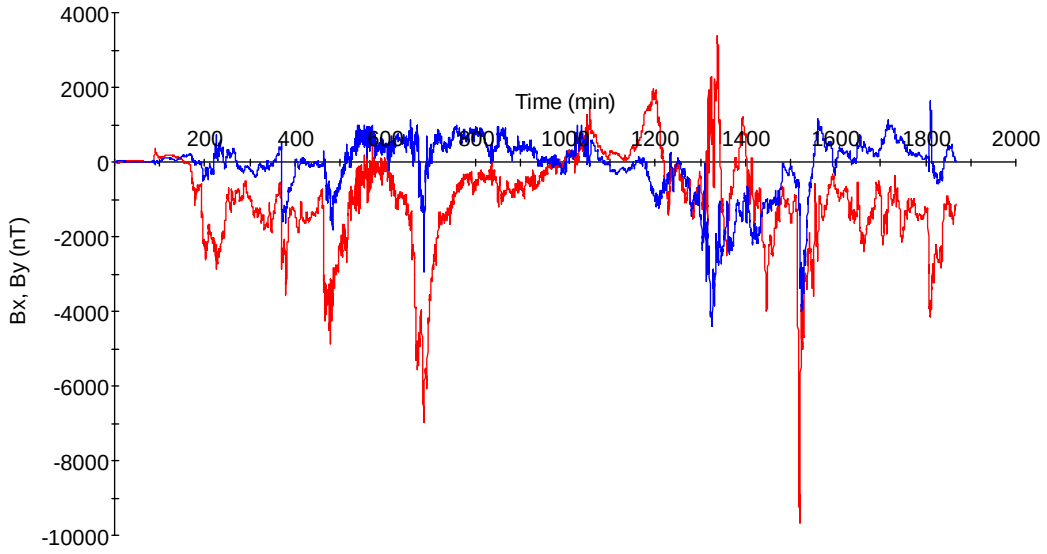


Figure 6: Supplemental Geomagnetic Field Waveform
Red B_N (Northward), Blue B_E (Eastward)

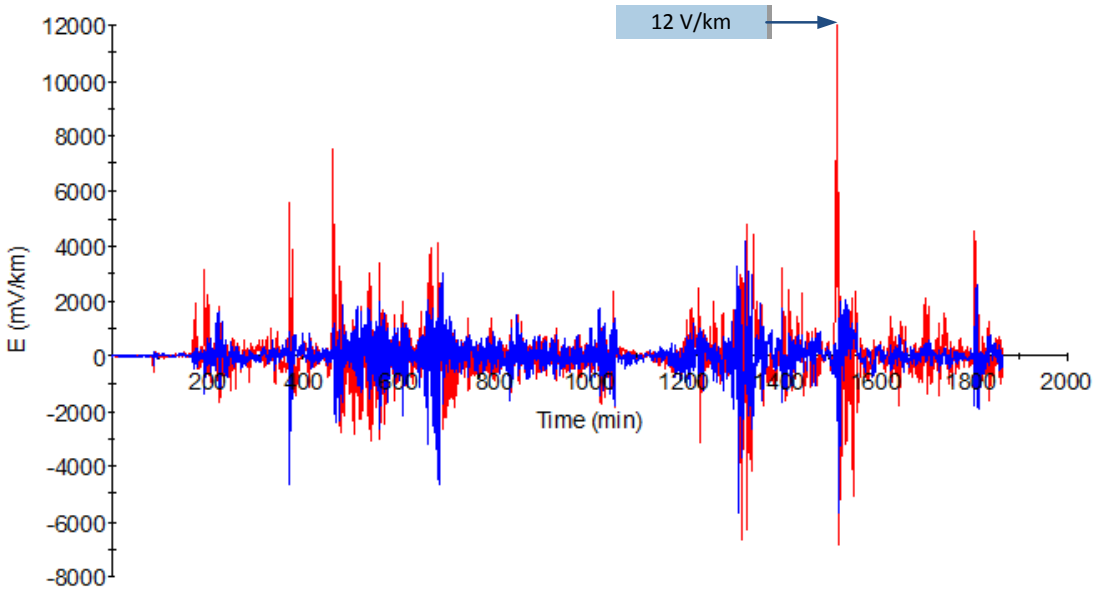


Figure 7: Supplemental Geoelectric Field Waveform
Blue E_N (Northward), Red E_E (Eastward)

Attachment 1-CAN

Attachment 1-CAN provides an alternative that a Canadian entity may use in lieu of the benchmark or supplemental GMD event(s) defined in Attachment 1 for performing GMD Vulnerability Assessment(s).

A Canadian entity may use the provisions of Attachment 1-CAN if it has regionally specific information that provides a technically justified means to re-define a 1-in-100 year GMD planning event(s) within its planning area.

Information for the Alternative Methodology

GMD Vulnerability Assessment(s) require the use of geophysical and engineering models. Canadian-specific data is available and growing. Ongoing research allows for more accurate characterization of regional parameters used in these models. Such Canadian-specific data includes geomagnetic field, earth conductivity, and geomagnetically induced current measurements that can be used for modeling and simulation validation.

Information used to calculate geoelectric fields for the benchmark and supplemental GMD events shall be clearly documented and technically justified. For example, the factors involved in the calculation of geoelectric fields are geomagnetic field variations and an earth transfer function(s).[1] Technically justified information used in modelling geomagnetic field variations may include: technical documents produced by governmental entities such as Natural Resources Canada; technical papers published in peer-reviewed journals; and data sets gathered using sound scientific principles. An earth transfer function may rely on magnetotelluric measurements or earth conductivity models.

Modeling assumptions shall also be clearly documented and technically justified. An entity may use sensitivity analysis to identify how the assumptions affect the results.

A simplified model may be used to perform a GMD Vulnerability Assessment(s), as long as the model is more conservative than a more detailed model.

When interpreting assessment results, the entity shall consider the maturity of the modeling, toolset, and techniques applied.

Geomagnetic Disturbance Planning Events

The 1-in-100 year planning event shall be based on regionally specific data and technically justifiable statistical analyses (e.g., extreme value theory) and applied to the benchmark and supplemental GMD Vulnerability Assessment(s).

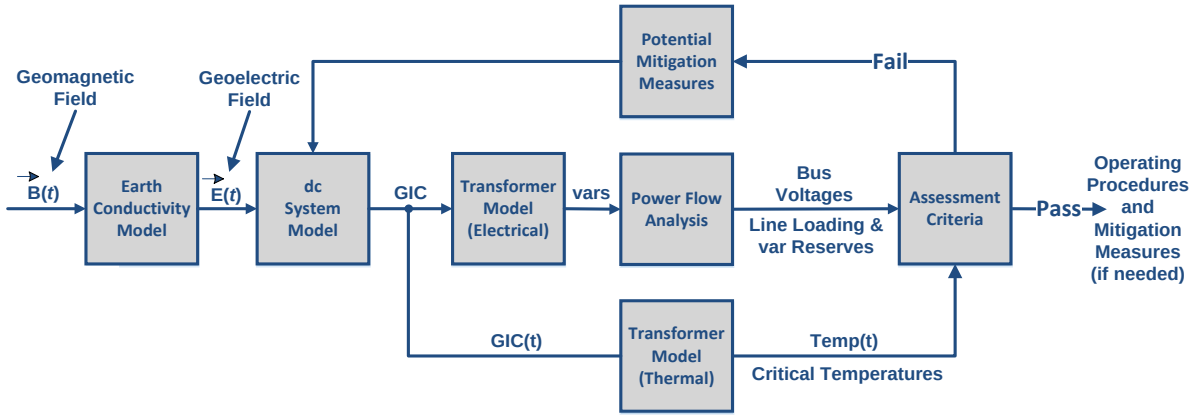
For the benchmark GMD Vulnerability Assessment(s), an entity shall consider the large-scale spatial structure of the GMD event. For the supplemental GMD Vulnerability Assessment(s), an

[1] The "earth transfer function" is the relationship between the electric fields and magnetic field variations at the surface of the earth.

entity shall consider the small-scale spatial structure of the GMD event (e.g., using magnetometer measurements or realistic electrojet calculations).

Guidelines and Technical Basis

The diagram below provides an overall view of the GMD Vulnerability Assessment process:



The requirements in this standard cover various aspects of the GMD Vulnerability Assessment process.

Benchmark GMD Event (Attachment 1)

The benchmark GMD event defines the geoelectric field values used to compute GIC flows that are needed to conduct a benchmark GMD Vulnerability Assessment. The *Benchmark Geomagnetic Disturbance Event Description*, May 2016[11] white paper includes the event description, analysis, and example calculations.

Supplemental GMD Event (Attachment 1)

The supplemental GMD event defines the geoelectric field values used to compute GIC flows that are needed to conduct a supplemental GMD Vulnerability Assessment. The *Supplemental Geomagnetic Disturbance Event Description*, October 2017[12] white paper includes the event description and analysis.

Requirement R2

A GMD Vulnerability Assessment requires a GIC System model, which is a dc representation of the System, to calculate GIC flow. In a GMD Vulnerability Assessment, GIC simulations are used to determine transformer Reactive Power absorption and transformer thermal response. Details for developing the GIC System model are provided in the NERC GMD Task Force guide: *Application Guide for Computing Geomagnetically-Induced Current in the Bulk Power System*, December 2013.[13]

Underground pipe-type cables present a special modeling situation in that the steel pipe that encloses the power conductors significantly reduces the geoelectric field induced into the

[11] http://www.nerc.com/pa/stand/Pages/TPL0071RI.aspx.
[12] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.
[13] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf.

conductors themselves, while they remain a path for GIC. Solid dielectric cables that are not enclosed by a steel pipe will not experience a reduction in the induced geoelectric field. A planning entity should account for special modeling situations in the GIC system model, if applicable.

Requirement R4

The *Geomagnetic Disturbance Planning Guide*,[14] December 2013 developed by the NERC GMD Task Force provides technical information on GMD-specific considerations for planning studies.

Requirement R5

The benchmark thermal impact assessment of transformers specified in Requirement R6 is based on GIC information for the benchmark GMD Event. This GIC information is determined by the planning entity through simulation of the GIC System model and must be provided to the entity responsible for conducting the thermal impact assessment. GIC information should be provided in accordance with Requirement R5 each time the GMD Vulnerability Assessment is performed since, by definition, the GMD Vulnerability Assessment includes a documented evaluation of susceptibility to localized equipment damage due to GMD.

The maximum effective GIC value provided in Part 5.1 is used for the benchmark thermal impact assessment. Only those transformers that experience an effective GIC value of 75 A or greater per phase require evaluation in Requirement R6.

GIC(t) provided in Part 5.2 is used to convert the steady state GIC flows to time-series GIC data for the benchmark thermal impact assessment of transformers. This information may be needed by one or more of the methods for performing a benchmark thermal impact assessment. Additional information is in the following section and the *Transformer Thermal Impact Assessment White Paper*,[15] October 2017.

The peak GIC value of 75 Amps per phase has been shown through thermal modeling to be a conservative threshold below which the risk of exceeding known temperature limits established by technical organizations is low.

Requirement R6

The benchmark thermal impact assessment of a power transformer may be based on manufacturer-provided GIC capability curves, thermal response simulation, thermal impact screening, or other technically justified means. Approaches for conducting the assessment are presented in the *Transformer Thermal Impact Assessment White Paper ERO Enterprise-Endorsed*

[14] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf.

[15] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

Implementation Guidance[16] for this requirement. This ERO-Endorsed document is posted on the NERC Compliance Guidance[17] webpage.

Transformers are exempt from the benchmark thermal impact assessment requirement if the effective GIC value for the transformer is less than 75 A per phase, as determined by a GIC analysis of the System. Justification for this criterion is provided in the *Screening Criterion for Transformer Thermal Impact Assessment White Paper*,[18] October 2017. A documented design specification exceeding this value is also a justifiable threshold criterion that exempts a transformer from Requirement R6.

The benchmark threshold criteria and its associated transformer thermal impact must be evaluated on the basis of effective GIC. Refer to the white papers for additional information.

Requirement R7

Technical considerations for GMD mitigation planning, including operating and equipment strategies, are available in Chapter 5 of the *Geomagnetic Disturbance Planning Guide*,[19] December 2013. Additional information is available in the *2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk-Power System*,[20] February 2012.

Requirement R8

The *Geomagnetic Disturbance Planning Guide*,[21] December 2013 developed by the NERC GMD Task Force provides technical information on GMD-specific considerations for planning studies.

The supplemental GMD Vulnerability Assessment process is similar to the benchmark GMD Vulnerability Assessment process described under Requirement R4.

Requirement R9

The supplemental thermal impact assessment specified of transformers in Requirement R10 is based on GIC information for the supplemental GMD Event. This GIC information is determined by the planning entity through simulation of the GIC System model and must be provided to the entity responsible for conducting the thermal impact assessment. GIC information should be provided in accordance with Requirement R9 each time the GMD Vulnerability Assessment is performed since, by definition, the GMD Vulnerability Assessment includes a documented evaluation of susceptibility to localized equipment damage due to GMD.

---

[16] http://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/TPL-007-1_Transformer_Thermal_Impact_Assessment_White_Paper.pdf.
[17] http://www.nerc.com/pa/comp/guidance/Pages/default.aspx.
[18] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.
[19] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf.
[20] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2012GMD.pdf.
[21] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf.

The maximum effective GIC value provided in Part 9.1 is used for the supplemental thermal impact assessment. Only those transformers that experience an effective GIC value of 85 A or greater per phase require evaluation in Requirement R10.

GIC(t) provided in Part 9.2 is used to convert the steady state GIC flows to time-series GIC data for the supplemental thermal impact assessment of transformers. This information may be needed by one or more of the methods for performing a supplemental thermal impact assessment. Additional information is in the following section.

The peak GIC value of 85 Amps per phase has been shown through thermal modeling to be a conservative threshold below which the risk of exceeding known temperature limits established by technical organizations is low.

Requirement R10

The supplemental thermal impact assessment of a power transformer may be based on manufacturer-provided GIC capability curves, thermal response simulation, thermal impact screening, or other technically justified means. Approaches for conducting the assessment are presented in the *Transformer Thermal Impact Assessment White Paper ERO Enterprise-Endorsed Implementation Guidance*[22] discussed in the Requirement R6 section above. A later version of the *Transformer Thermal Impact Assessment White Paper*,[23] October 2017, has been developed to include updated information pertinent to the supplemental GMD event and supplemental thermal impact assessment.

Transformers are exempt from the supplemental thermal impact assessment requirement if the effective GIC value for the transformer is less than 85 A per phase, as determined by a GIC analysis of the System. Justification for this criterion is provided in the revised *Screening Criterion for Transformer Thermal Impact Assessment White Paper*,[24] October 2017. A documented design specification exceeding this value is also a justifiable threshold criterion that exempts a transformer from Requirement R10.

The supplemental threshold criteria and its associated transformer thermal impact must be evaluated on the basis of effective GIC. Refer to the white papers for additional information.

Requirement R11

Technical considerations for GIC monitoring are contained in Chapter 6 of the *2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk-Power System*,[25] February 2012. GIC monitoring is generally performed by Hall effect transducers that are attached to the neutral of the wye-grounded transformer. Data from GIC monitors is useful for model validation and situational awareness.

---

[22] http://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/TPL-007-1_Transformer_Thermal_Impact_Assessment_White_Paper.pdf.
[23] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.
[24] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.
[25] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2012GMD.pdf.

Responsible entities consider the following in developing a process for obtaining GIC monitor data:

- **Monitor locations.** An entity's operating process may be constrained by location of existing GIC monitors. However, when planning for additional GIC monitoring installations consider that data from monitors located in areas found to have high GIC based on system studies may provide more useful information for validation and situational awareness purposes. Conversely, data from GIC monitors that are located in the vicinity of transportation systems using direct current (e.g., subways or light rail) may be unreliable.

- **Monitor specifications.** Capabilities of Hall effect transducers, existing and planned, should be considered in the operating process. When planning new GIC monitor installations, consider monitor data range (e.g., -500 A through + 500 A) and ambient temperature ratings consistent with temperatures in the region in which the monitor will be installed.

- **Sampling Interval.** An entity's operating process may be constrained by capabilities of existing GIC monitors. However, when possible specify data sampling during periods of interest at a rate of 10 seconds or faster.

- **Collection Periods.** The process should specify when the entity expects GIC data to be collected. For example, collection could be required during periods where the Kp index is above a threshold, or when GIC values are above a threshold. Determining when to discontinue collecting GIC data should also be specified to maintain consistency in data collection.

- **Data format.** Specify time and value formats. For example, Greenwich Mean Time (GMT) (MM/DD/YYYY HH:MM:SS) and GIC Value (Ampere). Positive (+) and negative (-) signs indicate direction of GIC flow. Positive reference is flow from ground into transformer neutral. Time fields should indicate the sampled time rather than system or SCADA time if supported by the GIC monitor system.

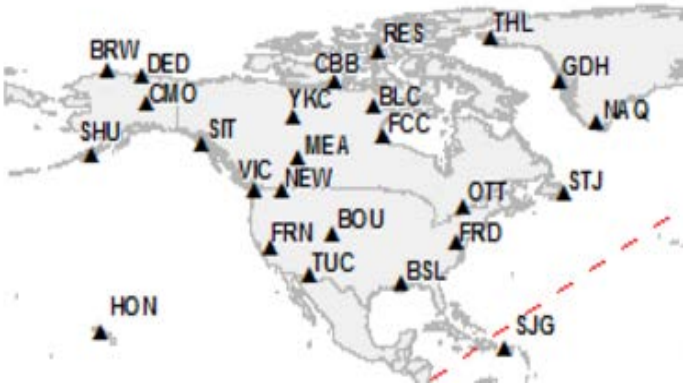
- **Data retention.** The entity's process should specify data retention periods, for example 1 year. Data retention periods should be adequately long to support availability for the entity's model validation process and external reporting requirements, if any.

- **Additional information.** The entity's process should specify collection of other information necessary for making the data useful, for example monitor location and type of neutral connection (e.g., three-phase or single-phase).

Requirement R12

Magnetometers measure changes in the earth's magnetic field. Entities should obtain data from the nearest accessible magnetometer. Sources of magnetometer data include:

- Observatories such as those operated by U.S. Geological Survey and Natural Resources Canada, see figure below for locations:[26]



- Research institutions and academic universities;
- Entities with installed magnetometers.

Entities that choose to install magnetometers should consider equipment specifications and data format protocols contained in the latest version of the *INTERMAGNET Technical Reference Manual*, Version 4.6, 2012.[27]

[26] http://www.intermagnet.org/index-eng.php.
[27] http://www.intermagnet.org/publications/intermag_4-6.pdf.

Rationale

During development of TPL-007-1, text boxes were embedded within the standard to explain the rationale for various parts of the standard. The text from the rationale text boxes was moved to this section upon approval of TPL-007-1 by the NERC Board of Trustees. In developing TPL-007-2, the SDT has made changes to the sections below only when necessary for clarity. Changes are marked with brackets [ ].

Rationale for Applicability:

Instrumentation transformers and station service transformers do not have significant impact on geomagnetically-induced current (GIC) flows; therefore, these transformers are not included in the applicability for this standard.

Terminal voltage describes line-to-line voltage.

Rationale for R1:

In some areas, planning entities may determine that the most effective approach to conduct a GMD Vulnerability Assessment is through a regional planning organization. No requirement in the standard is intended to prohibit a collaborative approach where roles and responsibilities are determined by a planning organization made up of one or more Planning Coordinator(s).

Rationale for R2:

A GMD Vulnerability Assessment requires a GIC System model to calculate GIC flow which is used to determine transformer Reactive Power absorption and transformer thermal response. Guidance for developing the GIC System model is provided in the *Application Guide Computing Geomagnetically-Induced Current in the Bulk-Power System*,[28] December 2013, developed by the NERC GMD Task Force.

The System model specified in Requirement R2 is used in conducting steady state power flow analysis that accounts for the Reactive Power absorption of power transformer(s) due to GIC in the System.

The GIC System model includes all power transformer(s) with a high side, wye-grounded winding with terminal voltage greater than 200 kV. The model is used to calculate GIC flow in the network.

The projected System condition for GMD planning may include adjustments to the System that are executable in response to space weather information. These adjustments could include, for example, recalling or postponing maintenance outages.

The Violation Risk Factor (VRF) for Requirement R2 is changed from Medium to High. This change is for consistency with the VRF for approved standard TPL-001-4 Requirement R1, which is proposed for revision in the NERC filing dated August 29, 2014 (Docket No. RM12-1-000). NERC guidelines require consistency among Reliability Standards.

[28] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf.

Rationale for R3:
Requirement R3 allows a responsible entity the flexibility to determine the System steady state voltage criteria for System steady state performance in Table 1. Steady state voltage limits are an example of System steady state performance criteria.

Rationale for R4:
The GMD Vulnerability Assessment includes steady state power flow analysis and the supporting study or studies using the models specified in Requirement R2 that account for the effects of GIC. Performance criteria are specified in Table 1.

At least one System On-Peak Load and at least one System Off-Peak Load must be examined in the analysis.

Distribution of GMD Vulnerability Assessment results provides a means for sharing relevant information with other entities responsible for planning reliability. Results of GIC studies may affect neighboring systems and should be taken into account by planners.

The *Geomagnetic Disturbance Planning Guide*,[29] December 2013 developed by the NERC GMD Task Force provides technical information on GMD-specific considerations for planning studies. The provision of information in Requirement R4, Part 4.3, shall be subject to the legal and regulatory obligations for the disclosure of confidential and/or sensitive information.

Rationale for R5:
This GIC information is necessary for determining the thermal impact of GIC on transformers in the planning area and must be provided to entities responsible for performing the thermal impact assessment so that they can accurately perform the assessment. GIC information should be provided in accordance with Requirement R5 as part of the GMD Vulnerability Assessment process since, by definition, the GMD Vulnerability Assessment includes documented evaluation of susceptibility to localized equipment damage due to GMD.

The maximum effective GIC value provided in Part 5.1 is used for transformer thermal impact assessment.

GIC(t) provided in Part 5.2 can alternatively be used to convert the steady state GIC flows to time-series GIC data for transformer thermal impact assessment. This information may be needed by one or more of the methods for performing a thermal impact assessment. Additional guidance is available in the *Transformer Thermal Impact Assessment White Paper*,[30] October 2017.

A Transmission Owner or Generator Owner that desires GIC(t) may request it from the planning entity. The planning entity shall provide GIC(t) upon request once GIC has been calculated, but

[29] http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf.
[30] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

no later than 90 calendar days after receipt of a request from the owner and after completion of Requirement R5, Part 5.1.

The provision of information in Requirement R5 shall be subject to the legal and regulatory obligations for the disclosure of confidential and/or sensitive information.

Rationale for R6:

The transformer thermal impact screening criterion has been revised from 15 A per phase to 75 A per phase [for the benchmark GMD event]. Only those transformers that experience an effective GIC value of 75 A per phase or greater require evaluation in Requirement R6. The justification is provided in the *Screening Criterion for Transformer Thermal Impact Assessment White Paper*,[31] October 2017.

The thermal impact assessment may be based on manufacturer-provided GIC capability curves, thermal response simulation, thermal impact screening, or other technically justified means. The transformer thermal assessment will be repeated or reviewed using previous assessment results each time the planning entity performs a GMD Vulnerability Assessment and provides GIC information as specified in Requirement R5. Approaches for conducting the assessment are presented in the *Transformer Thermal Impact Assessment White Paper*,[32] October 2017.

Thermal impact assessments are provided to the planning entity, as determined in Requirement R1, so that identified issues can be included in the GMD Vulnerability Assessment (R4), and the Corrective Action Plan (R7) as necessary.

Thermal impact assessments of non-BES transformers are not required because those transformers do not have a wide-area effect on the reliability of the interconnected Transmission system.

The provision of information in Requirement R6, Part 6.4, shall be subject to the legal and regulatory obligations for the disclosure of confidential and/or sensitive information.

Rationale for R7:

The proposed requirement addresses directives in Order No. 830 for establishing Corrective Action Plan (CAP) deadlines associated with GMD Vulnerability Assessments. In Order No. 830, FERC directed revisions to TPL-007 such that CAPs are developed within one year from the completion of GMD Vulnerability Assessments (P 101). Furthermore, FERC directed establishment of implementation deadlines after the completion of the CAP as follows (P 102):

- Two years for non-hardware mitigation; and
- Four years for hardware mitigation.

The objective of Part 7.4 is to provide awareness to potentially impacted entities when implementation of planned mitigation is not achievable within the deadlines established in Part

[31] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.
[32] http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx.

7.3. Examples of situations beyond the control of the of the responsible entity (see Section 7.4) include, but are not limited to:

- Delays resulting from regulatory/legal processes, such as permitting;
- Delays resulting from stakeholder processes required by tariff;
- Delays resulting from equipment lead times; or

Delays resulting from the inability to acquire necessary Right-of-Way.

Rationale for Table 3:

Table 3 has been revised to use the same ground model designation, FL1, as is being used by USGS. The calculated scaling factor for FL1 is 0.74. [The scaling factor associated with the benchmark GMD event for the Florida earth model (FL1) has been updated to 0.76 in TPL-007-2 based on the earth model published on the USGS public website.]

Rationale for R8 – R10:

The proposed requirements address directives in Order No. 830 for revising the benchmark GMD event used in GMD Vulnerability Assessments (P 44, P 47-49). The requirements add a supplemental GMD Vulnerability Assessment based on the supplemental GMD event that accounts for localized peak geoelectric fields.

Rationale for R11 – R12:

The proposed requirements address directives in Order No. 830 for requiring responsible entities to collect GIC monitoring and magnetometer data as necessary to enable model validation and situational awareness (P 88; P. 90-92). GMD measurement data refers to GIC monitor data and geomagnetic field data in Requirements R11 and R12, respectively. See the Guidelines and Technical Basis section of this standard for technical information.

The objective of Requirement R11 is for entities to obtain GIC data for the Planning Coordinator's planning area or other part of the system included in the Planning Coordinator's GIC System model to inform GMD Vulnerability Assessments. Technical considerations for GIC monitoring are contained in Chapter 9 of the *2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk-Power System* (NERC 2012 GMD Report). GIC monitoring is generally performed by Hall effect transducers that are attached to the neutral of the transformer and measure dc current flowing through the neutral.

The objective of Requirement R12 is for entities to obtain geomagnetic field data for the Planning Coordinator's planning area to inform GMD Vulnerability Assessments. Magnetometers provide geomagnetic field data by measuring changes in the earth's magnetic field. Sources of geomagnetic field data include:

- Observatories such as those operated by U.S. Geological Survey, Natural Resources Canada, research organizations, or university research facilities;
- Installed magnetometers; and
- Commercial or third-party sources of geomagnetic field data.

Geomagnetic field data for a Planning Coordinator's planning area is obtained from one or more of the above data sources located in the Planning Coordinator's planning area, or by obtaining a geomagnetic field data product for the Planning Coordinator's planning area from a government or research organization. The geomagnetic field data product does not need to be derived from a magnetometer or observatory within the Planning Coordinator's planning area.

VAR-001-5

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-5

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

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

B. Requirements and Measures

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operations planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operations Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include, but is not limited to, instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

R4. Each Transmission Operator shall specify the criteria that will exempt generators: 1) from following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt: 1) from following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target

value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures M1 through M6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operations Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R4 and R5. Please note that Requirement R4 is deleted and R5 is replaced with the following requirements.

Requirements and Measures

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

M.E.A.13 Each Transmission Operator will have evidence that it provided the voltage schedules to the Generator Operator, as required in E.A.13. Evidence may include, but is not limited to, dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

M.E.A.14 The Transmission Operator will have evidence that it provided one of the voltage schedule reference points for each generation resource in its area to the Generator Operator, as required in E.A.14. Evidence may include, but is not limited to dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource.

E.A.15 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals

within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M.E.A.15 The Generator Operator will have evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals, as required in E.A.15. Evidence may include, but is not limited to, dated reports, spreadsheets, or other documentation.

E.A.16 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M.E.A.16 The Transmission Operator will have evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology, as required in E.A.16. Evidence may include, but is not limited to, dated reports, spreadsheets, or other documentation.

E.A.17 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the automatic voltage regulators (AVR) to manage Mvar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.17.1 Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.17.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

M.E.A.17 If the Generator Operator uses outside control loops to manage Mvar loading, the Generator Operator will have evidence that it met the control loop specifications in sub-parts E.A.17.1 through E.A.17.2, as required in E.A.17 and its sub-parts. Evidence may include, but is not limited to, design specifications with identified agreed-upon control loops, system reports, or other dated documentation.

Violation Severity Levels

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.13	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to at least one generation resource but less than or equal to 5% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 5% but less than or equal to 10% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 10% but less than or equal to 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.
E.A.14	The Transmission Operator did not provide a voltage schedule reference point for at least one but less than or equal to 5% of the generation resources in the Transmission Operator area.	The Transmission Operator did not provide a voltage schedule reference point for more than 5% but less than or equal to 10% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not a voltage schedule reference point for more than 10% but less than or equal to 15% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not provide a voltage schedule reference point for more than 15% of the generation resources in the Transmission Operator Area.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.15	The Generator Operator provided its voltage set point conversion methodology greater than 30 days but less than or equal to 60 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Transmission Operator.	The Generator Operator did not provide its voltage set point conversion methodology within 120 days of a request by the Transmission Operator.
E.A.16	The Transmission Operator provided its data to support development of the voltage set point conversion methodology than 30 days but less than or equal to 60 days of a request by the Generator Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Generator. Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Generator. Operator.	The Transmission Operator did not provide its data to support development of the voltage set point conversion methodology within 120 days of a request by the Generator Operator.
E.A.17	N/A	The Generator Operator did not meet the control loop specifications in E.A.17.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in E.A.17.1 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in E.A.17.1 through E.A.17.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.

E. Interpretations

None

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	June 18, 2007	FERC approved Version 1 of the standard.	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	August 5, 2010	Adopted by NERC Board of Trustees; Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised
2	January 10, 2011	FERC issued letter order approving the addition of LSEs and Controllable Load to the standard.	Revised
3	May 9, 2012	Adopted by NERC Board of Trustees; Modified to add a WECC region variance	Revised
3	June 20, 2013	FERC issued order approving VAR-001-3	Revised
3	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	Revised
4	February 6, 2014	Adopted by NERC Board of Trustees	Revised
4	August 1, 2014	FERC issued letter order issued approving VAR-001-4	
4.1	August 25, 2015	Added “or” to Requirement R5, 5.3 to read: schedules or Reactive Power	Errata
4.1	November 13, 2015	FERC Letter Order approved errata to VAR-001-4.1. Docket RD15-6-000	Errata
4.2	June 14, 2017	Project 2016-EPR-02 errata recommendations	Errata
4.2	August 10, 2017	Adopted by NERC Board of Trustees	Errata
4.2	September 26, 2017	FERC Letter Order issued approving VAR-001-4.2 Docket No. RD17-7-000.	
5	August 16, 2018	Adopted by NERC Board of Trustees	1) In E.A.14 “Area” was changed to

			"area."; 2) E.A.15 and associated elements were eliminated; 3) Measures were updated and relocated matching current conventions, replacing "shall" with "will"; 4) typographical errors in VSL Table for E.A.17 were corrected; 5) format was updated.
5	10/15/2018	FERC Order issued approving VAR-001-5 Docket No. RD18-8-000.	

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

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

Rationale for R1:

Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) voltage stability ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency voltage limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: VAR-001-5 — Voltage and Reactive Control

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
VAR-001-5	All	01/01/2019		

Printed On: January 07, 2019, 10:23 AM

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-01 Canadian-Specific Revisions to TPL-007-2

Applicable Standard(s)

- TPL-007-3- Transmission System Planned Performance for Geomagnetic Disturbance Events

Requested Retirement(s)

- TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events
- TPL-007-2 – Transmission System Planned Performance for Geomagnetic Disturbance Events

Prerequisite Standard(s)

None

Applicable Entities

- Planning Coordinator with a planning area that includes a Facility or Facilities specified in Section 4.2 of the standard;
- Transmission Planner with a planning area that includes a Facility or Facilities specified in Section 4.2 of the standard;
- Transmission Owner who owns a Facility or Facilities specified in Section 4.2 of the standard; and
- Generator Owner who owns a Facility or Facilities specified in Section 4.2 of the standard.

Section 4.2 states that the standard applies to facilities that include power transformer(s) with a high side, wye-grounded winding with terminal voltage greater than 200 kV.

Terms in the NERC Glossary of Terms

There are no new, modified, or retired terms.

Background

In January 2018, NERC submitted for regulatory approval Reliability Standard TPL-007-2. This standard was developed in response to certain directives of the United States Federal Energy Regulatory Commission (FERC) from Order No. 830 (September 22, 2016), approving Reliability Standard TPL-007-1 and its associated five-year Implementation Plan and directing certain modifications.

In May 2018, a Standard Authorization Request was submitted identifying a need for a Canadian-specific Variance to the TPL-007-2 standard. Specifically, the Standard Authorization Request sought to provide an option for Canadian Registered Entities to define alternative Benchmark GMD Events and/or Supplemental GMD Events specific to their unique topology.

Reliability Standard TPL-007-3 adds a Variance for Canadian entities. The Canadian Variance replaces, in its entirety, Requirement R7, Part 7.3 of the continent-wide standard for Canadian entities and adds an alternate methodology for GMD Vulnerability Assessments, as described in Attachment 1-CAN. None of the continent-wide Requirements have been changed.

Effective Date and Phased-In Compliance Dates

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

Reliability Standard TPL-007-3

United States

The standard shall become effective on the later of: (1) the effective date of Reliability Standard TPL-007-2; or (2) the first day of the first calendar quarter after the date TPL-007-3 is adopted by the NERC Board of Trustees.

This implementation plan incorporates by reference the phased-in compliance dates of the TPL-007-2 implementation plan (see Attachment 1).

All Other Jurisdictions

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

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

This implementation plan incorporates by reference the phased-in compliance dates of the TPL-007-2 implementation plan (see Attachment 1), except that the phased-in compliance dates described therein shall be based on the effective date of TPL-007-3.

Attachment 1-
TPL-007-2 Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2013-03 Geomagnetic Disturbance Mitigation
Reliability Standard TPL-007-2

Applicable Standard

- TPL-007-2 - Transmission System Planned Performance for Geomagnetic Disturbance Events

Requested Retirement

- TPL-007-1 - Transmission System Planned Performance for Geomagnetic Disturbance Events

Prerequisite Standard

None

Applicable Entities

- *Planning Coordinator with a planning area that includes a Facility or Facilities specified in Section 4.2 of the standard;*
- *Transmission Planner with a planning area that includes a Facility or Facilities specified in Section 4.2 of the standard;*
- *Transmission Owner who owns a Facility or Facilities specified in Section 4.2 of the standard; and*
- *Generator Owner who owns a Facility or Facilities specified in Section 4.2 of the standard*.

Section 4.2 states that the standard applies to facilities that include power transformer(s) with a high-side, wye-grounded winding with terminal voltage greater than 200 kV.

Terms in the NERC Glossary of Terms

There are no new, modified, or retired terms.

Background

On September 22, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 830 approving Reliability Standard TPL-007-1 and its associated five-year Implementation Plan. In the Order, FERC also directed NERC to develop certain modifications to the standard. FERC established a deadline of 18 months from the effective date of Order No. 830 for completing the revisions, which is May 2018.

General Considerations

This Implementation Plan is intended to integrate the new requirements in TPL-007-2 with the GMD Vulnerability Assessment process that is being implemented through approved TPL-007-1. At the time of the May 2018 filing deadline, many requirements in approved standard TPL-007-1 that lead

to completion of the geomagnetic disturbance (GMD) Vulnerability Assessment will be in effect. Furthermore, many entities may be taking steps to complete studies or assessments that are required by future enforceable requirements in TPL-007-1. The Implementation Plan phases in the requirements in TPL-007-2 based on the effective date of TPL-007-2, as follows:

- **Effective Date before January 1, 2021**. Implementation timeline supports applicable entities completing new requirements for supplemental GMD Vulnerability Assessments concurrently with requirements for the benchmark GMD Vulnerability Assessment (concurrent effective dates).

- **Effective Date on or after January 1, 2021**. Implementation timeline supports applicable entities completing the benchmark GMD Vulnerability Assessments before new requirements for supplemental GMD Vulnerability Assessments become effective.

Effective Date

The effective date for the proposed Reliability Standard is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of the proposed Reliability Standard (e.g., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. These phased-in compliance dates represent the dates that entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Standard TPL-007-2

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

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

Phased-In Compliance Dates

If TPL-007-2 becomes effective before January 1, 2021

Implementation timeline supports applicable entities completing new requirements for supplemental GMD Vulnerability Assessments concurrently with requirements for the benchmark GMD Vulnerability Assessment (concurrent effective dates).

Compliance Date for TPL-007-2 Requirements R1 and R2

Entities shall be required to comply with Requirements R1 and R2 upon the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R5
Entities shall not be required to comply with Requirements R5 until six (6) months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R9
Entities shall not be required to comply with Requirement R9 until six (6) months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirements R11 and R12
Entities shall not be required to comply with Requirements R11 and R12 until 24 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirements R6 and R10
Entities shall not be required to comply with Requirements R6 and R10 until 30 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirements R3, R4, and R8
Entities shall not be required to comply with Requirements R3, R4, and R8 until 42 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R7
Entities shall not be required to comply with Requirement R7 until 54 months after the effective date of Reliability Standard TPL-007-2.

If TPL-007-2 becomes effective on or after January 1, 2021

Implementation timeline supports applicable entities completing the benchmark GMD Vulnerability Assessments before new requirements for supplemental GMD Vulnerability Assessments become effective.

Compliance Date for TPL-007-2 Requirements R1, R2, R5, and R6
Entities shall be required to comply with Requirements R1, R2, R5, and R6 upon the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirements R3 and R4
Entities shall not be required to comply with Requirements R3 and R4 until 12 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirements R7, R11, and R12
Entities shall not be required to comply with Requirements R7, R11, and R12 until 24 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R9
Entities shall not be required to comply with Requirement R9 until 36 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R10
Entities shall not be required to comply with Requirement R10 until 60 months after the effective date of Reliability Standard TPL-007-2.

Compliance Date for TPL-007-2 Requirement R8
Entities shall not be required to comply with Requirement R8 until 72 months after the effective date of Reliability Standard TPL-007-2.

Retirement Date

Standard TPL-007-1
Reliability Standard TPL-007-1 shall be retired immediately prior to the effective date of TPL-007-2 in the particular jurisdiction in which the revised standard is becoming effective.

Initial Performance of Periodic Requirements

Transmission Owners and Generator Owners are not required to comply with Requirement R6 prior to the compliance date for Requirement R6, regardless of when geomagnetically-induced current (GIC) flow information specified in Requirement R5, Part 5.1 is received.

Transmission Owners and Generator Owners are not required to comply with Requirement R10 prior to the compliance date for Requirement R10, regardless of when GIC flow information specified in Requirement R9, Part 9.1 is received.

Exhibit B: List of Currently Effective NERC Reliability Standards

Resource and Demand Balancing (BAL)	
BAL-001-2	Real Power Balancing Control Performance
BAL-001-TRE-1	Primary Frequency Response in the ERCOT Region
BAL-002-2(i)	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event
BAL-002-WECC-2a	Contingency Reserve
BAL-003-1.1	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
Communications (COM)	
COM-001-3	Communications
COM-002-4	Operating Personnel Communications Protocols
Critical Infrastructure Protection (CIP)	
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-6	Cyber Security — Security Management Controls
CIP-004-6	Cyber Security — Personnel & Training
CIP-005-5	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-008-5	Cyber Security — Incident Reporting and Response Planning
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security — Information Protection
CIP-014-2	Physical Security
Emergency Preparedness and Operations (EOP)	
EOP-004-3	Event Reporting

EOP-005-2	System Restoration from Blackstart Resources
EOP-006-2	System Restoration Coordination
EOP-008-1	Loss of Control Center Functionality
EOP-010-1	Geomagnetic Disturbance Operations
EOP-011-1	Emergency Operations
Facilities Design, Connections, and Maintenance (FAC)	
FAC-001-3	Facility Interconnection Requirements
FAC-002-2	Facility Interconnection Studies
FAC-003-4	Transmission Vegetation Management
FAC-008-3	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-013-2	Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon
FAC-014-2	Establish and Communicate System Operating Limits
FAC-501-WECC-2	Transmission Maintenance
Interchange Scheduling and Coordination (INT)	
INT-004-3.1	Dynamic Transfers
INT-006-4	Evaluation of Interchange Transactions
INT-009-2.1	Implementation of Interchange
INT-010-2.1	Interchange Initiation and Modification for Reliability
Interconnection Reliability Operations and Coordination (IRO)	
IRO-001-4	Reliability Coordination – Responsibilities
IRO-002-5	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-TRE-1	IROL and SOL Mitigation in the ERCOT Region
IRO-006-WECC-2	Qualified Transfer 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-010-2	Reliability Coordinator Data Specification and Collection
IRO-014-3	Coordination Among Reliability Coordinators
IRO-017-1	Outage Coordination
IRO-018-1(i)	Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities
Modeling, Data, and Analysis (MOD)	
MOD-001-1a	Available Transmission System Capability
MOD-004-1	Capacity Benefit Margin
MOD-008-1	Transmission Reliability Margin Calculation Methodology
MOD-020-0	Providing Interruptible Demands and Direct Control Load Management Data to System Operators and Reliability Coordinators
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-031-2	Demand and Energy Data
MOD-032-1	Data for Power System Modeling and Analysis
MOD-033-1	Steady-State and Dynamic System Model Validation
Nuclear (NUC)	
NUC-001-3	Nuclear Plant Interface Coordination
Personnel Performance, Training, and Qualifications (PER)	
PER-003-1	Operating Personnel Credentials
PER-004-2	Reliability Coordination — Staffing
PER-005-2	Operations Personnel Training
Protection and Control (PRC)	
PRC-001-1.1(ii)	System Protection Coordination
PRC-002-2	Disturbance Monitoring and Reporting Requirements
PRC-004-5(i)	Protection System Misoperation Identification and Correction

PRC-004-WECC-2	Protection System and Remedial Action Scheme Misoperation
PRC-005-1.1b	Transmission and Generation Protection System Maintenance and Testing
PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance
PRC-006-3	Automatic Underfrequency Load Shedding
PRC-006-NPCC-1	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-015-1	Remedial Action Scheme Data and Documentation
PRC-016-1	Remedial Action Scheme Misoperations
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
Transmission Operations (TOP)	
TOP-001-4	Transmission Operations
TOP-002-4	Operations Planning
TOP-003-3	Operational Reliability Data
TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities
Transmission Planning (TPL)	
TPL-001-4	Transmission System Planning Performance Requirements
TPL-007-1	Transmission System Planned Performance for Geomagnetic Disturbance Events
Voltage and Reactive (VAR)	

VAR-001-5	Voltage and Reactive Control
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 July 3, 2018

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 July 3, 2018.

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 following: **sarcomm@nerc.net** with "Glossary Comment" in the subject line.

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 minimum vegetation clearance distances.
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. (*From FERC order 888-A.*)
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 Balancing Authorities in the Western Interconnection.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 generally reported on an area to area basis.
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.
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	Version 0 Reliability Standards	AGC	2/8/2005	3/16/2007		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.
Automatic Time Error Correction (I_{ATEC}) ***continued below...***	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	The addition of a component to the ACE equation for the Western Interconnection that modifies the control point for the purpose of continuously paying back Primary Inadvertent Interchange to correct accumulated time error. Automatic Time Error Correction is only applicable in the Western Interconnection. $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H}$ when operating in Automatic Time error correction Mode.The absolute value of I_{ATEC} shall not exceed L_{max}. I_{ATEC} shall be zero when operating in any other AGC mode. • L_{max} is the maximum value allowed for I_{ATEC} set by each BA between $0.2*\|B_i\|$ and L10, $0.2*\|B_i\| \le L_{max} \le L10$. • $L_{10} = 1.65 * \varepsilon_{10} \sqrt{(-10B_i)(-10B_S)}$. • ε10 is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-minute average frequency error based on frequency performance over a given year. The bound, ε 10, is the same for every Balancing Authority Area within an Interconnection.
Automatic Time Error Correction (I_{ATEC})	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	• Y = Bi / BS. • 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} - Bi * 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: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t)*(TE_{offset})$

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Automatic Time Error Correction (I_{ATEC})	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	• 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: $\mathbf{PII}_{accum}^{on/offpeak} = last\ period's\ \mathbf{PII}_{accum}^{on/offpeak} + \mathbf{PII}_{hourly}$
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	Version 0 Reliability Standards	BA	2/8/2005	3/16/2007		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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Balancing Contingency Event	Project 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	Any single event described in Subsections (A), (B), or (C) below, or any series of such otherwise single events, with each separated from the next by one minute or less. A. Sudden loss of generation: a. Due to i. unit tripping, or ii. loss of generator Facility resulting in isolation of the generator from the Bulk Electric System or from the responsible entity's System, or iii. sudden unplanned outage of transmission Facility; b. And, that causes an unexpected change to the responsible entity's ACE; B. Sudden loss of an Import, due to forced outage of transmission equipment that causes an unexpected imbalance between generation and Demand on the Interconnection. C. Sudden restoration of a Demand that was used as a resource that causes an unexpected change to the responsible entity's ACE.
Base Load	Version 0 Reliability		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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 Imple-mentation Plan for Phase 2 Compliance obligations.)	Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. **Inclusions:** • I1 - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded by application of Exclusion E1 or E3. • I2 – Generating resource(s) including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above with: a) Gross individual nameplate rating greater than 20 MVA. Or, b) Gross plant/facility aggregate nameplate rating greater than 75 MVA. • I3 - Blackstart Resources identified in the Transmission Operator's restoration plan.

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 Imple-mentation Plan for Phase 2 Compliance obligations.)	• 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: 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 Imple-mentation Plan for Phase 2 Compliance obligations.)	**Exclusions:** • **E1** - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusions I2, I3, or I4, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or, c) Where the radial system serves Load and includes generation resources, not identified in Inclusions I2, I3 or I4, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating). Note 1 – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion. Note 2 – The presence of a contiguous loop, operated at a voltage level of 50 kV or less, between configurations being considered as radial systems, does not affect this exclusion.
Bulk Electric System **(continued)**	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Imple-mentation Plan for Phase 2 Compliance obligations.)	• **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 Imple-mentation Plan for Phase 2 Compliance obligations.)	• **E3** - Local networks (LN): A group of contiguous transmission Elements operated at less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN's emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customers and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following: a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusions I2, I3, or I4 and do not have an aggregate capacity of non-retail generation greater than 75 MVA (gross nameplate rating); b) Real Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and
Bulk Electric System **(continued)**	Project 2010-17	BES	11/21/2013	3/20/2014	7/1/2014 (Please see the Imple-mentation 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). • 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 capability preserved as CBM is intended to be used by the LSE only in times of emergency generation deficiencies.
Capacity Benefit Margin Implementation Document	Project 2006-07	CBMID	11/13/2008	11/24/2009		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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	The provision of capacity that may be deployed by the Balancing Authority to respond to a Balancing Contingency Event and other contingency requirements (such as Energy Emergency Alerts as specified in the associated EOP standard). A Balancing Authority may include in its restoration of Contingency Reserve readiness to reduce Firm Demand and include it if, and only if, the Balancing Authority: • is experiencing a Reliability Coordinator declared Energy Emergency Alert level, and is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan. • is utilizing its Contingency Reserve to mitigate an operating emergency in accordance with its emergency Operating Plan.
Contingency Reserve Restoration Period	Project 2010-14.1 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.
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
Cyber Security Incident	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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* : • 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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 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.
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.
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.
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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).
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		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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	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.
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.
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.
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		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Low Impact BES Cyber System Electronic Access Point	Project 2014-02	LEAP	2/12/2015	1/21/2016	7/1/2016	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	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).
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	The failure of a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation: **1. Failure to Trip – During Fault** – A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct. **2. Failure to Trip – Other Than Fault** – A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct. **3. Slow Trip – During Fault** – A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System. (continued below…)
Misoperation (continued…)	Project 2010-05.1		8/14/2014	5/13/2015	7/1/2016	**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. **5. Unnecessary Trip – During Fault** – An unnecessary Composite Protection System operation for a Fault condition on another Element. **6. Unnecessary Trip – Other Than Fault** – An unnecessary Composite Protection System operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 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.
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 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.
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.
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.)

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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: • Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.
Operating Reserve – Supplemental	Version 0 Reliability Standards		2/8/2005	3/16/2007		The portion of Operating Reserve consisting of: • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.
Operating Voltage	Project 2007-07		2/7/2006	3/16/2007		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
Protection System	Project 2007-17 Protection System Maintenance and Testing		11/19/2010	2/3/2012	4/1/2013	Protection System – • 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 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: • 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Pseudo-Tie	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 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).
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
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.
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.
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 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.)

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
Remedial Action Scheme	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	A scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and Mvar), tripping load, or reconfiguring a System(s). RAS accomplish objectives such as: • Meet requirements identified in the NERC Reliability Standards; • Maintain Bulk Electric System (BES) stability; • Maintain acceptable BES voltages; • Maintain acceptable BES power flows; • Limit the impact of Cascading or extreme events. The following do not individually constitute a RAS: a. Protection Systems installed for the purpose of detecting Faults on BES Elements and isolating the faulted Elements 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

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Remedial Action Scheme ***Continued***	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	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 ***Continued***	Project 2010-05.2	RAS	11/13/2014	11/19/2015	4/1/2017	n. Generator controls such as, but not limited to, automatic generation control (AGC), generation excitation [e.g. automatic voltage regulation (AVR) and power system stabilizers (PSS)], fast valving, and speed governing
Removable Media	Project 2014-02		2/12/2015	1/21/2016	7/1/2016	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.
Reportable Balancing Contingency Event	Project 2010-14.1 Phase 1		11/5/2015	1/19/2017	1/1/2018	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. • Eastern Interconnection – 900 MW • Western Interconnection – 500 MW • ERCOT – 800 MW • Quebec – 500 MW

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
Reportable Cyber Security Incident	Project 2008-06 Cyber Security Order 706_V5 CIP Standards		11/26/2012	11/22/2013	7/1/2016	A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.
Reportable Disturbance	Version 0 Reliability Standards		2/8/2005	3/16/2007		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.
Reporting ACE	Project 2010-14.2.1. Phase 2		2/11/2016		7/1/2016	The scan rate values of a Balancing Authority Area's (BAA) Area Control Error (ACE) measured in MW includes the difference between the Balancing Authority Area's Actual Net Interchange and its Scheduled Net Interchange, plus its Frequency Bias Setting obligation, plus correction for any known meter error. In the Western Interconnection, Reporting ACE includes Automatic Time Error Correction (ATEC). Reporting ACE is calculated as follows: Reporting ACE = $(NI_A - NI_S) - 10B (F_A - FS) - I_{ME}$ 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. • 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	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: 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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 aforementioned 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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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"
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
System Operating Limit	Project 2015-04 Alignment of Terms	SOL	11/5/2015	1/21/2016	7/1/2016	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: • 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.
Telemetering	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.
Tie Line	Version 0		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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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 *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g* enerally equal to the transfer capability from "Area B" to "Area A."
Transfer Distribution Factor	Version 0 Reliability Standards		2/8/2005	3/16/2007		See Distribution Factor.
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	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	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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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.
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.

SUBJECT TO ENFORCEMENT						
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Definition**
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**
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.
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.
Operational Planning Analysis	Project 2007-06.2 Phase 2 of System Protection Coordination	OPA	8/11/2016	6/7/2018	10/1/2020	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.)
Protection System Coordination Study	Project 2007-06 System Protection Coordination		11/5/2015	6/7/2018	10/1/2020	An analysis to determine whether Protection Systems operate in the intended sequence during Faults.
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).
Real-time Assessment	Project 2007-06.2 Phase 2 of System Protection Coordination	RTA	8/11/2016		10/1/2020	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.)

PENDING 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	Storage media that: 1. are not Cyber Assets, 2. are capable of transferring executable code, 3. can be used to store, copy, move, or access data, and 4. are directly connected for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • Protected Cyber Asset associated with high or medium impact BES Cyber Systems. Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset	Project 2016-02 Modifications to CIP Standards	TCA	2/9/2017	4/19/2018	1/1/2020	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

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			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			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))
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.
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
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.
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	Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. Inclusions: • I1 - Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded 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 Electric System **(Continued)**	Project 2010-17	BES	1/18/2012	6/14/2013		Replaced by BES definition FERC approved 3/20/2014	**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. **Exclusions:** • **E1** - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: a) Only serves Load. Or, b) Only includes generation resources, not identified in 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). Note – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion.

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	• **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	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-Power System	Project 2012-08.1 Phase 1		5/9/2013	7/9/2013		6/30/2016	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.

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 11/24/2009			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 Trasfer Capabilites		11/1/2006 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 pre-determined 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.
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
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.
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.

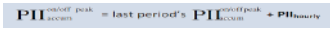
Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Interconnection Reliability Operating Limit	Version 0 Reliability Standards	IROL	2/8/2005	3/16/2007		12/27/2007	The value (such 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.
Misoperation	Phase III - IV Planning Standards - Archive		2/7/2006	3/16/2007		6/30/2016	• 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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Postback	Project 2006-07 ATC/TTC/AFC and CBM/TRM Revisions		8/22/2008	Not approved; Modification directed 11/24/09			Positive adjustments to ATC or AFC as defined in Business Practices. Such Business Practices may include processing of redirects and unscheduled service.
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
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
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
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.
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Remedial Action Scheme	Version 0 Reliability Standards	RAS	2/8/2005	3/16/2007		3/31/2017	See "Special Protection System"
Reporting Ace			8/15/2013	4/16/2015 (Will not go into effect)			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). 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.
Reporting Ace **(Continued)**			8/15/2013	4/16/2015 (Will not go into effect)			**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. $_{ATEC}$ shall be zero when opera $I_{ATEC} = \frac{PII_{\text{most recent hour}}}{(1-Y) * H}$ when operating in Automatic Time Error Correction control mode. • Y = B / BS. • H = Number of hours used to payback Primary Inadvertent Interchange energy. The value of H is set to 3.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
Reporting Ace **(Continued)**							energy. The value of H is set to 3. B_S = Frequency Bias for the Interconnection (MW / 0.1 Hz). • 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. Where:  All NERC Interconnections with multiple Balancing Authorities operate using the
Reporting Ace **(Continued)**			8/15/2013	4/16/2015 (Will not go into effect)			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. 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.)
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.

Retired Terms							
Continent-wide Term	**Link to Project Page**	**Acronym**	**BOT Adoption Date**	**FERC Approval Date**	**Effective Date**	**Inactive Date**	**Definition**
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: • 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.
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	Transmission Vegetation		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		An event that results in a Frequency Deviation, identified at the BA's sole discretion, and meeting one of the following conditions: i) a Frequency Deviation that has a pre-perturbation [the 16-second period of time before t(0)] average frequency to post-perturbation [the 32-second period of time starting 20 seconds after t(0)] average frequency absolute deviation greater than 100 mHz (the 100 mHz value may be adjusted by the BA to capture 30 to 40 events per year). Or ii) a cumulative change in generating unit/generating facility, DC tie and/or firm load pre-perturbation megawatt value to post-perturbation megawatt value absolute deviation greater than 550 MW (the 550 MW value may be adjusted by the BA to capture 30 to 40 events per year).
Governor			8/15/2013	1/16/2014	4/1/2014		The electronic, digital or mechanical device that implements Primary Frequency Response of generating units/generating facilities or other system elements.
Primary Frequency Response	BAL-001-TRE-1 Implementation Plan	PFR	8/15/2013	1/16/2014	4/1/2014		The immediate proportional increase or decrease in real power output provided by generating units/generating facilities and the natural real power dampening response provided by Load in response to system Frequency Deviations. This response is in the direction that stabilizes frequency.

WECC REGIONAL DEFINITIONS							
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			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: *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).*

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: • 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			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 Transfer Path	WECC Regional Standards Under Development		2/10/2009	3/17/2011			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			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 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		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			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**
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