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

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

FIRST QUARTER 2016 APPLICATION FOR APPROVAL OF RELIABILITY STANDARDS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
Senior Counsel
Andrew C. Wills
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charles.berardesco@nerc.net
shamai.elstein@nerc.net
andrew.wills@nerc.net

Counsel for the North American Electric Reliability Corporation

May 26, 2016

TABLE OF CONTENTS

EXHIBITS

Exhibit A –

1.) Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

2.) Informational Summary of Each Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

3.) Reliability Standards Filed for Approval

Exhibit B – List of Currently Effective NERC Reliability Standards

Exhibit C – Updated *Glossary of Terms Used in NERC Reliability Standards*

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

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

FIRST QUARTER 2016 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 NERC Reliability Standards and an updated *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary" or "Glossary") approved by the United States Federal Energy Regulatory Commission ("FERC" or the "Commission") during the first quarter of 2016. This filing covers the time period from January 1, 2016, through March 31, 2016. NERC requests that, as specified herein, these Reliability Standards and the associated NERC Glossary be made mandatory and enforceable for users, owners, and operators of the Bulk-Power System within the Province of Nova Scotia.

In support of this request, NERC submits the following information: (1) a table showing effective dates of each Reliability Standard applicable to Nova Scotia that was approved by FERC in the first quarter of 2016 (**Exhibit A1**), (2) an informational summary of each Reliability Standard applicable to Nova Scotia that was approved by FERC in the first quarter of 2016, including each standard's purpose, applicability, and filing and approval dates (**Exhibit A2**), (3) Reliability Standards approved by FERC in the first quarter of 2016 (**Exhibit A3**); and (4) an updated list of the currently effective NERC Reliability Standards and the associated updated

NERC Glossary, as approved by the Commission (see **Exhibit B** and **Exhibit C**, respectively).[1]

I. NOTICES AND COMMUNICATIONS

Notices and communications regarding this application may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
Senior Counsel
Andrew C. Wills
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charles.berardesco@nerc.net
shamai.elstein@nerc.net
andrew.wills@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,[2] NERC has been certified by the Commission as the Electric Reliability Organization ("ERO") in the United States.[3] The Reliability Standards contained in **Exhibit A3** have been approved by the Commission as mandatory and enforceable for users, owners, and operators of the Bulk-Power System within the United States. Some or all of NERC's Reliability Standards are also mandatory in the Canadian provinces of Alberta, British Columbia, Manitoba, New Brunswick, Nova Scotia,

[1] NERC notes that the list of Reliability Standards and NERC Glossary in **Exhibit B** and **Exhibit C** 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) (2012) (entrusting FERC with the duties of approving and enforcing rules in the U.S. to ensure the reliability of the Nation's bulk power system, and with the duties of certifying an Electric Reliability Organization to develop mandatory and enforceable Reliability Standards, subject to FERC review and approval).

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

Ontario, Québec, and Saskatchewan.

NERC entered into a Memorandum of Understanding ("MOU") with the NSUARB,[4] and a separate MOU with Nova Scotia Power Incorporated ("NSPI") and the Northeast Power Coordinating Council, Inc. ("NPCC"),[5] to provide reliability services to Nova Scotia. These MOUs became effective on December 22, 2006, and May 11, 2010, respectively. The December 22, 2006, MOU memorializes the relationship between NERC and the NSUARB formed to improve the reliability of the North American Bulk-Power System. 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, and on July 20, 2011, NSUARB issued a decision approving these documents.[6] In that decision, the NSUARB approved a "quarterly review" process for considering new and amended NERC Reliability Standards and criteria[7] and ordered that "applications will not be processed by the Board until [FERC] has approved or remanded the standards in the United States."[8] The NSUARB Decision also stated that NSUARB approval is not required for Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") associated with proposed Reliability Standards, but the NSUARB noted that it will accept VRFs

---

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

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

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

7 *Id.* at P 30.

8 *Id*.

and VSLs as guidance.[9]

Based on the NSUARB Decision, NERC applications to the NSUARB only request approval for those Reliability Standards and 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 below to the FERC-approved VRFs and VSLs associated with NERC Reliability Standards.[10] NERC does not include in its applications the full developmental record for the standards, which consists of the draft standards, comments received, responses to the comments by the drafting teams, and the full voting record, because the record for each standard may consist of several thousand pages. NERC will make the full developmental records available to the NSUARB or other interested parties upon request.

B. Overview of NERC Reliability Standards Development Process

NERC Reliability Standards define the requirements for reliably planning and operating the North American Bulk-Power System. 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 the balloting process, have approved the standards provided in **Exhibit A3**, and the standards have been adopted by the NERC Board of Trustees.

NERC develops Reliability Standards and associated definitions in accordance with Section 300 (Reliability Standards Development) and Appendix 3A (Standards Processes

---

[9] *Id*. at P 33.

[10] 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.

Manual) of its Rules of Procedure.[11] 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 May 17, 2016, 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. NERC submits the NERC Glossary as **Exhibit C** of this application for informational purposes.

C. Description of Proposed Definitions and Reliability Standards, 1st Quarter 2016

As explained in more detail below, the Commission issued the following orders in the first quarter of 2016 approving NERC Reliability Standards and revising certain implementation dates: (1) a letter order approving 26 revised definitions issued on January 21, 2016;[12] (2) an order approving seven Critical Infrastructure Protection (CIP) Reliability Standards issued on January 21, 2016,[13] and a related order delaying implementation of CIP version 5 Reliability Standards for certain entities,[14] (3) a letter order approving Reliability Standard MOD-031-2 issued on February 18, 2016;[15] and (4) an order approving Reliability Standard PRC-026-1 issued on March 17, 2016. [16]

---

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

[12] *N. Am. Elec. Reliability Corp.*, Docket No. RD16-3-000 (Jan. 21, 2016) (unpublished letter order). NERC also notes that, on the same day, FERC approved revisions to definitions for 16 terms in Appendix 2 of the NERC Rules of Procedure as part of a coordinated effort to align the terms with the revisions to the NERC Glossary of Terms submitted in the abovementioned FERC Docket. *See N. Am. Elec. Reliability Corp.*, Docket No. RR16-2-000 (January 21, 2016) (unpublished letter order).

[13] *N. Am. Elec. Reliability Corp.*, Order No. 822, 154 FERC ¶ 61,037 (2016).

[14] *Order Granting Extension of Time*, Docket No. RM15-14-000, 154 FERC ¶ 61,137 (2016).

[15] *N. Am. Elec. Reliability Corp.*, Docket No. RD16-1-000 (Feb. 18, 2016) (unpublished letter order).

[16] *N. Am. Elec. Reliability Corp.*, Order No. 823, 154 FERC ¶ 61, 192 (2016).

Reliability Standard	Effective Date
Critical Infrastructure Protection (CIP) Standards[17]	
CIP-003-6*	7/1/2016
CIP-004-6*	7/1/2016
CIP-006-6*	7/1/2016
CIP-007-6*	7/1/2016
CIP-009-6*	7/1/2016
CIP-010-2*	7/1/2016
CIP-011-2*	7/1/2016
Modeling, Data, and Analysis (MOD) Standard	
MOD-031-2*	10/1/2016
Protection and Control (PRC) Standard	
PRC-026-1*	1/1/2018

*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.

1. Revised NERC Glossary Definitions

On January 21, 2016, FERC approved revisions to definitions of 26 terms to be included in the NERC Glossary, attached herein as **Exhibit C**, associated implementation plan, and retirement of the currently-effective definitions. The revisions were developed as part of a broader effort to align the definitions of terms in the Glossary with those in the NERC Rules of Procedure to ensure consistency and reduce confusion in the application of defined terms across the ERO enterprise. As NERC requested that the Commission approve the modifications to the NERC Glossary contemporaneously with associated revisions to the NERC Rules of Procedure, FERC simulatenously approved corresponding revisions to the Rules of Procedure definitions to effectuate the proposed alignment.[18]

[17] NERC notes that, on February 25, 2016, FERC granted an extension of time to defer the implementation of CIP version 5 Reliability Standards from April 1, 2016, to July 1, 2016 to align with the implementation dates for the CIP Reliability Standards approved on January 21, 2016 in Order No. 822. *See Order Granting Extension of Time,, supra* n. 14; *see also* Order No. 822, *supra* n. 13.

[18] *See*, *supra* n. 12.

2. Critical Infrastructure Protection (CIP) Reliability Standards

On January 21, 2016, the Commission issued Order No. 822 approving the following seven (7) proposed Reliability Standards ("CIP Reliability Standards"):

- CIP-003-6 — Cyber Security — Security Management Controls;
- CIP-004-6 — Cyber Security – Personnel & Training;
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems;
- CIP-007-6 — Cyber Security – Systems Security Management;
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems;
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments; and
- CIP-011-2 — Cyber Security — Information Protection.

Along with the associated Implementation Plan and VRFs and VSLs for each of the CIP Reliability Standards, the Commission also approved the retirement of the following seven (7) currently-effective Reliability Standards:

- CIP-003-5 — Cyber Security — Security Management Controls;
- CIP-004-5.1 — Cyber Security – Personnel & Training;
- CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems;
- CIP-007-5 — Cyber Security – Systems Security Management;
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems;
- CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments; and
- CIP-011-1 — Cyber Security — Information Protection.

Finally, the Commission approved new or revised definitions of the following six (6) NERC Glossary terms:

- BES Cyber Asset
- Protected Cyber Asset
- Low Impact Electronic Access Point
- Low Impact External Routable Connectivity
- Removable Media
- Transient Cyber Asset

The CIP Reliability Standards are designed to mitigate the cybersecurity risks to Bulk Electric System ("BES") Facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cyber-attack, would affect the reliable operation of the BES. The CIP Reliability Standards address the directives in Order No. 791[19] by: (1) eliminating the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements; (2) providing enhanced security controls for "Low Impact" assets; (3) providing controls to address the risks posed by transient electronic devices (e.g., thumb drives and laptop computers) used at "High Impact" and "Medium Impact" BES Cyber Systems; and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks." Taken together, the CIP Reliability Standards improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards.

Pursuant to the associated Implementation Plan, the CIP Reliability Standards approved in Order No. 822 will become effective on July 1, 2016, although compliance with certain of the added requirements is not required until April 1, 2017 or September 1, 2018. Because the prior

[19] *N. Am. Elec. Reliability Corp.*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

versions of those standards were poised to become effective on April 1, 2016, several trade organizations filed a motion requesting an extension of time to defer the implementation of those standard until July 1, 2016. On February 25, 2016, the Commission granted this request, stating that "separate implementation dates in short succession create unnecessary administrative burdens with little or no commensurate benefit to reliability."

3. MOD-031-2

On February 18, 2016, FERC approved Reliability Standard MOD-031-2 (Demand and Energy Data), the associated implementation plan and VRFs and VSLs, and the retirement of Reliability Standard MOD-031-1. Reliability Standard MOD-031-2 is an improvement to the existing version of the standard because it clarifies the compliance obligations related to (1) providing data to Regional Entities and (2) responding to a request for data subject to confidentiality restrictions. Reliability Standard MOD-031-2 applies to Planning Authorities/Planning Coordinators,[20] Transmission Planners, Balancing Authorities, Resource Planners, Load-Serving Entities, and Distribution Providers.

4. PRC-026-1

On March 17, 2016, FERC approved Reliability Standard PRC-026-1 (Relay Performance During Stable Power Swings) and the associated implementation plan, VRFs, and VSLs. Reliability Standard PRC-026-1 is designed to ensure the use of protective relay systems that can differentiate between faults and stable power swings. Relatedly, the standard satisfies the directive in Order No. 733 related to undesirable relay operation because of power swings by prevent the unnecessary tripping of BES elements in response to stable power swings.

[20] See Section 4 of the Reliability Standard MOD-031-2 standard document, included herein in **Exhibit A3**, for a detailed explanation of the proposed synchronization of "Planning Authority" and "Planning Coordinator."

Reliability Standard PRC-026-1 applies to Planning Coordinators, Reliability Coordinators, Transmission Planners, and certain Generator Owners and Transmission Owners.[21]

[21] As noted in Section 4 of the Reliability Standard PRC-026-1 standard document, Reliability Standard PRC-026-1 applies to Generator Owners and Transmission Owners "that appl[y] load-responsive protective relays at the terminals of [Generators, Transformers, and Transmission Lines]."

III. CONCLUSION

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

Respectfully submitted,

/s/ *Andrew C. Wills*

Charles A. Berardesco
Senior Vice President and General Counsel
Shamai Elstein
Senior Counsel
Andrew C. Wills
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charles.berardesco@nerc.net
shamai.elstein@nerc.net
andrew.wills@nerc.net

Counsel for the North American Electric Reliability Corporation

Exhibit A (1): Reliability Standards Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

Reliability Standard	Effective Date
Critical Infrastructure Protection (CIP) Standards[1]	
CIP-003-6*	7/1/2016
CIP-004-6*	7/1/2016
CIP-006-6*	7/1/2016
CIP-007-6*	7/1/2016
CIP-009-6*	7/1/2016
CIP-010-2*	7/1/2016
CIP-011-2*	7/1/2016
Modeling, Data, and Analysis (MOD) Standard	
MOD-031-2*	10/1/2016
Protection and Control (PRC) Standard	
PRC-026-1*	1/1/2018

* 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.

[1] NERC notes that, on February 25, 2016, FERC granted an extension of time to defer the implementation of CIP version 5 Reliability Standards from April 1, 2016, to July 1, 2016 to align with the implementation dates for the CIP Reliability Standards approved on January 21, 2016 in Order No. 822. *See Order Granting Extension of Time*, *supra* n. 14; *see also* Order No. 822, *supra* n. 13.

Exhibit A (2)

Informational Summary of Each Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-003-6 - To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-003-6:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

Reliability Standard CIP-003-6 includes four requirements, several model tables providing reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP.

On February 13, 2015, the North American Electric Reliability Corporation ("NERC") NERC filed a petition for approval of proposed Reliability Standard CIP-003-6 (Cyber Security — Security Management Controls) with the Federal Energy Regulatory Commission ("FERC" or "Commission") in Docket No. RM15-14-000. The Commission approved CIP-003-6 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-004-6 - To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-004-6:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

Reliability Standard CIP-004-6 includes five requirements.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-004-6 (Cyber Security – Personnel & Training) with FERC in Docket No. RM15-14-000. The Commission approved CIP-004-6 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-006-6 - To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-006-6:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

Reliability Standard CIP-006-6 includes three requirements.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-006-6 (Cyber Security — Physical Security of BES Cyber Systems) with FERC in Docket No. RM15-14-000. The Commission approved CIP-006-6 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-007-6 - To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-007-6:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

Reliability Standard CIP-007-6 includes five requirements and one diagram.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-007-6 (Cyber Security – Systems Security Management) with FERC in Docket No. RM15-14-000. The Commission approved CIP-007-6 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-009-6 - To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-009-6:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

Reliability Standard CIP-009-6 includes three requirements and figures.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-009-6 (Cyber Security — Recovery Plans for BES Cyber Systems) with FERC in Docket No. RM15-14-000. The Commission approved CIP-009-6 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-010-2 - 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:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-010-2:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
        - Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

Reliability Standard CIP-010-2 includes four requirements.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-010-2 (Cyber Security — Configuration Change Management and Vulnerability Assessments) with FERC in Docket No. RM15-14-000. The Commission approved CIP-010-2 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

CIP-011-2 - To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Applicability:

- Functional Entities:
  - Balancing Authority
  - Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
    - 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.
    - Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
    - 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.
    - Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
  - Generator Operator
  - Generator Owner
  - Interchange Coordinator or Interchange Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Owner
- Facilities
  - 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:
    - Each UFLS or 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.

        - Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
        - 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.
        - 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.
    - Responsible Entities listed in 4.1 other than Distribution Providers:

      All BES Facilities.

    - Exemptions: The following are exempt from Standard CIP-011-2:
        - Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
        - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
        - 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.
        - For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.
        - Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

Reliability Standard CIP-011-2 includes two requirements.

On February 13, 2015, NERC filed a petition for approval of proposed Reliability Standard CIP-011-2 (Cyber Security — Information Protection) with FERC in Docket No. RM15-14-000. The Commission approved CIP-011-2 on January 21, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

MOD-031-2 - To provide authority for applicable entities to collect Demand, energy and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents of that data.

Applicability:

- Planning Authority and Planning Coordinator (hereafter collectively referred to as the "Planning Coordinator")
    - This proposed standard combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria list "Planning Authority," and they are not yet synchronized. Until that occurs, the proposed standard applies to both "Planning Authority" and "Planning Coordinator."
- Transmission Planner
- Balancing Authority
- Resource Planner
- Load-Serving Entity
- Distribution Provider

Reliability Standard MOD-031-2 includes four requirements.

On November 13, 2015, NERC filed a petition for approval of proposed Reliability Standard MOD-031-2 (Demand and Energy Data) with FERC in Docket No. RD16-1-000. The Commission approved MOD-031-2 on February 18, 2016.

Exhibit A (2): Informational Summary of Reliability Standard Applicable to Nova Scotia, Approved by FERC in First Quarter 2016

PRC-026-1 - To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.

Applicability:

- Generator Owner that applies load-responsive protective relays
- Planning Coordinator
- Transmission Owner that applies load-responsive protective relays
- Facilities: The following Elements that are part of the Bulk Electric System (BES):
    - Generators
    - Transformers
    - Transmission lines

Reliability Standard PRC-026-1 includes four requirements, ten figures and eight tables.

On December 31, 2014, NERC filed a petition for approval of proposed Reliability Standard PRC-026-1 (Relay Performance During Stable Power Swings) with FERC in Docket No. RM15-8-000. The Commission approved PRC-026-1 on March 17, 2016.

Exhibit A (3): Reliability Standards Filed for Approval

CIP-003-6 Reliability Standard

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

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

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

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 (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.

5. Effective Dates:

See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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.

B. Requirements and Measures

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

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

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

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

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

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2,	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to CIP-003-6,	The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to CIP-003-6,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	Requirement R2, Attachment 1, Section 2. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R3)	within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

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

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	

CIP-003-6 - Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing a LEAP.

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

- Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

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

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

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

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the 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:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-6, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through

successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

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

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

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

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse

or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or

control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems, including LEAPs. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term “electronic access control” is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “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,” such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “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." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and

other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

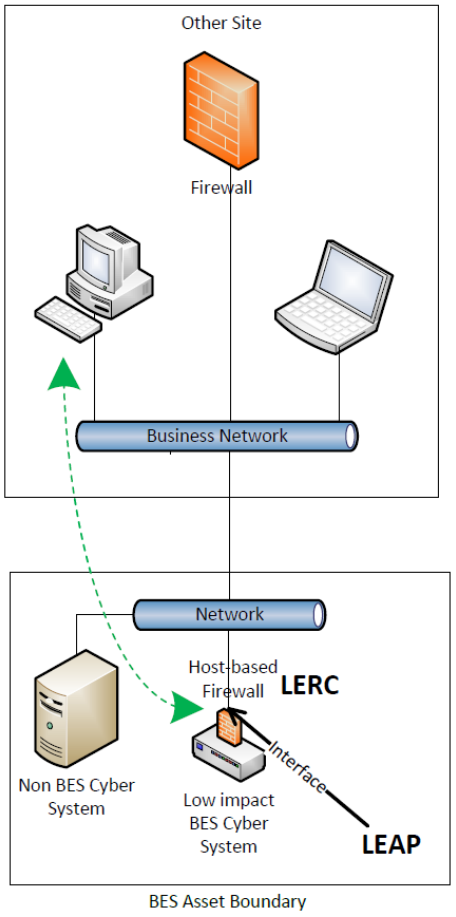
- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a “protocol break” so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

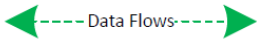
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would not meet the intent of “controlling” inbound and

outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

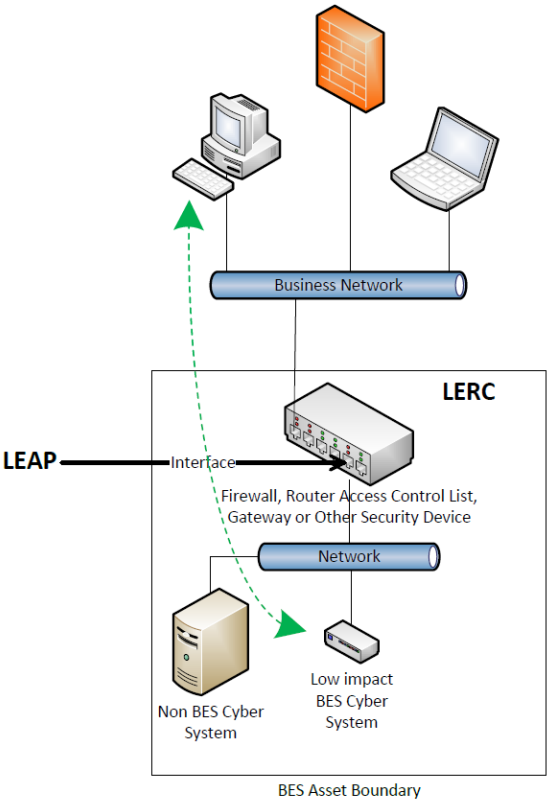
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.





REFERENCE MODEL - 1

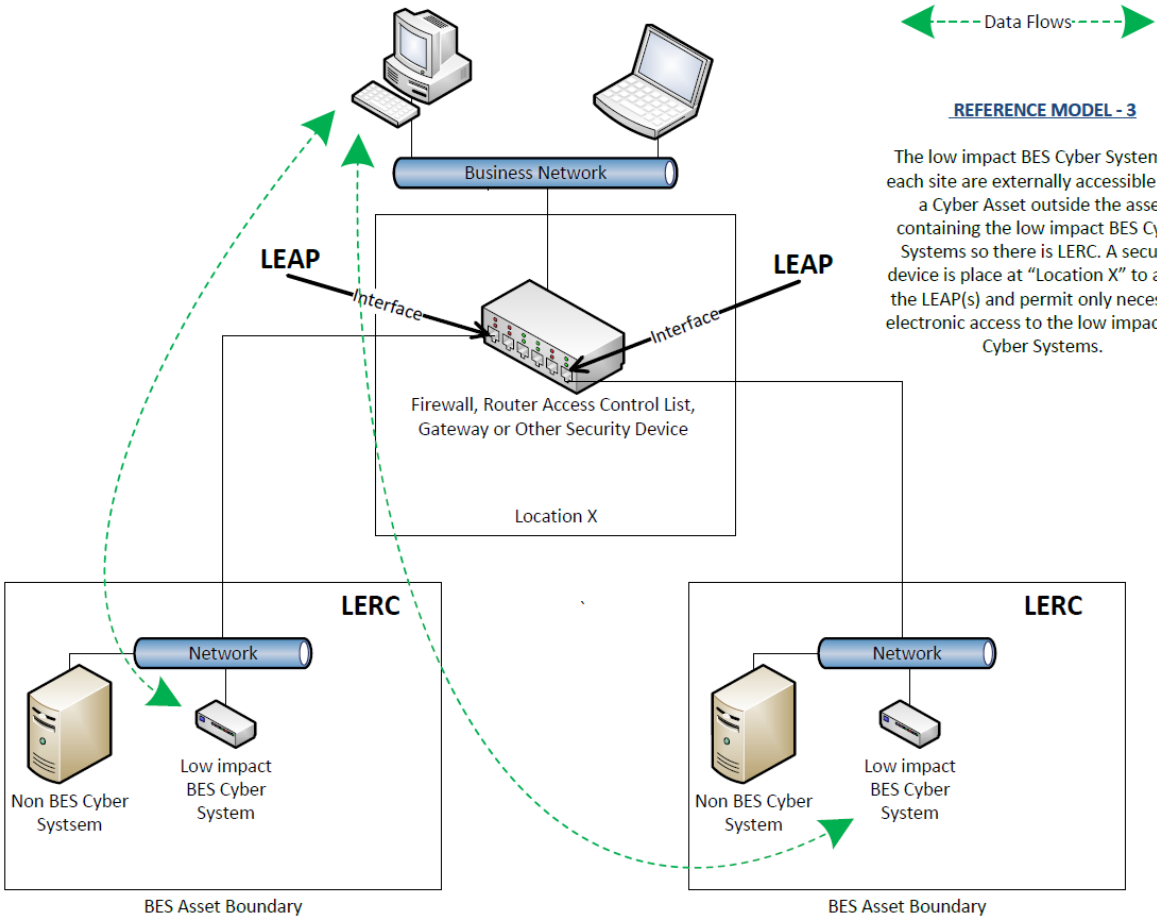
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

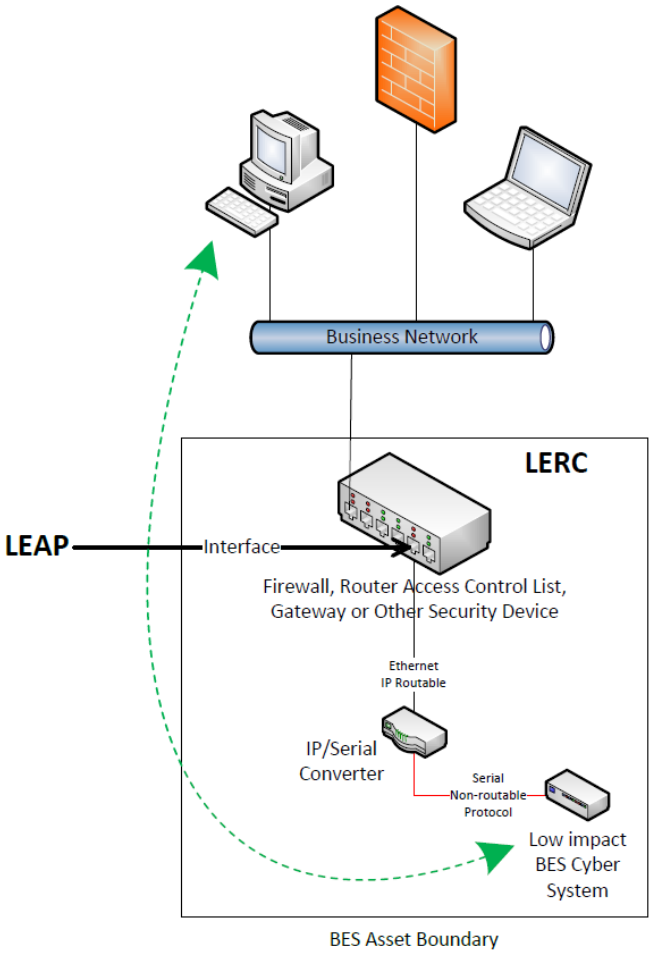


Data Flows

REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

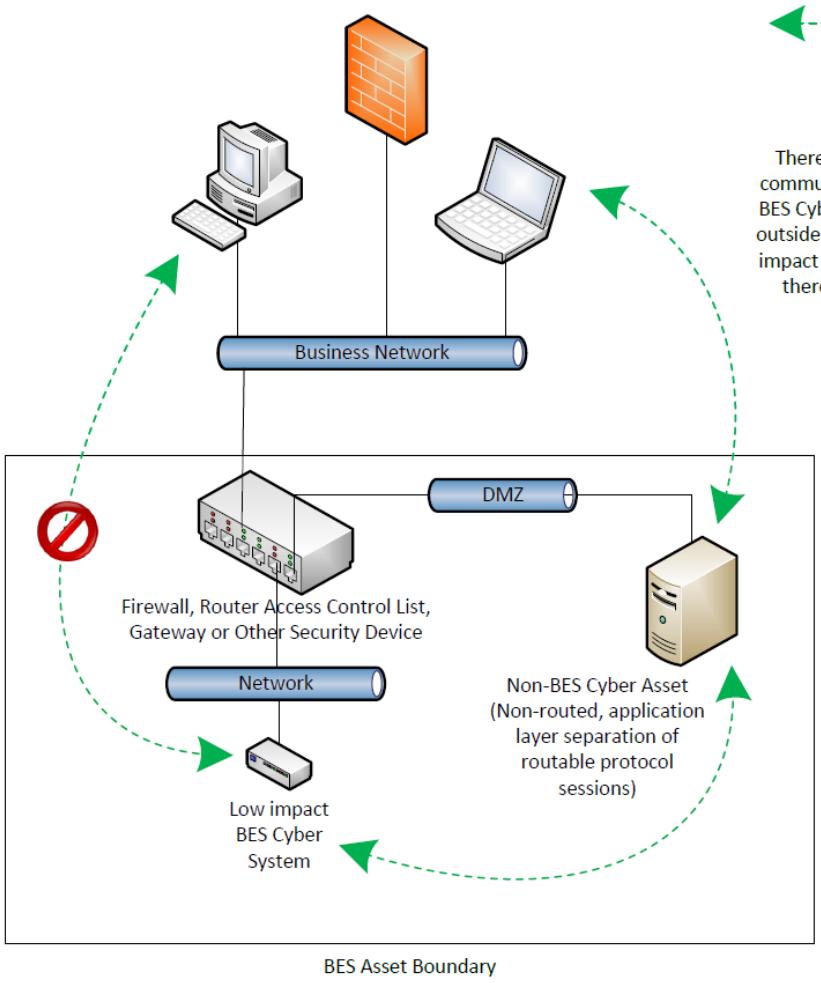

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

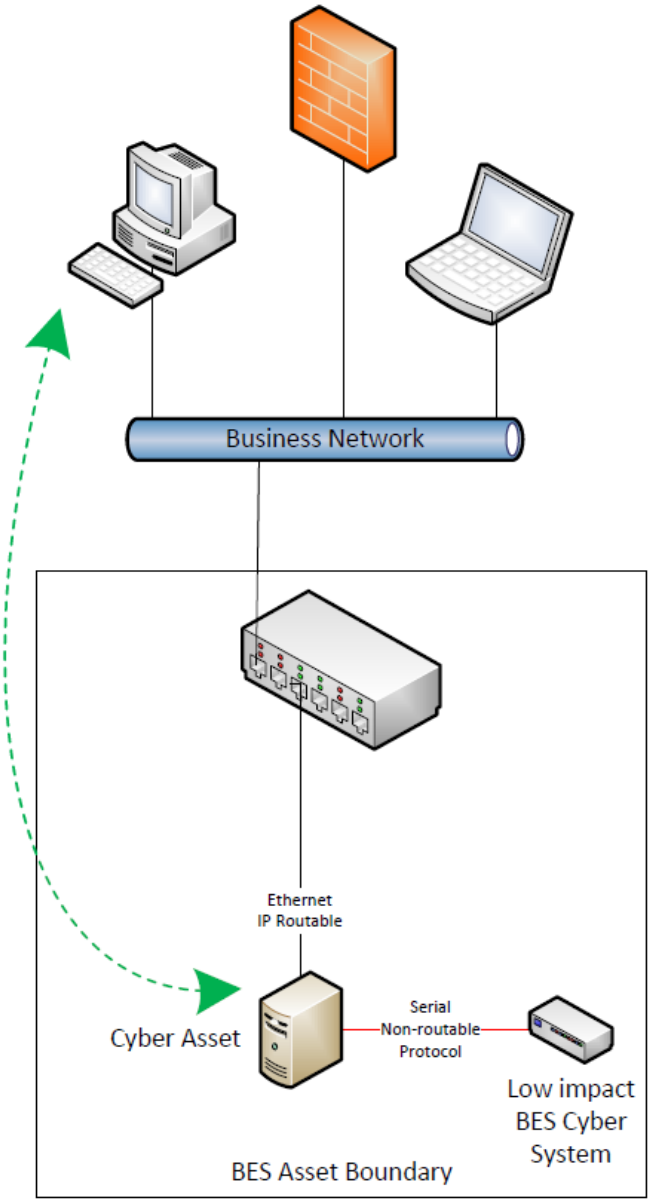


Data Flows

REFERENCE MODEL - 4

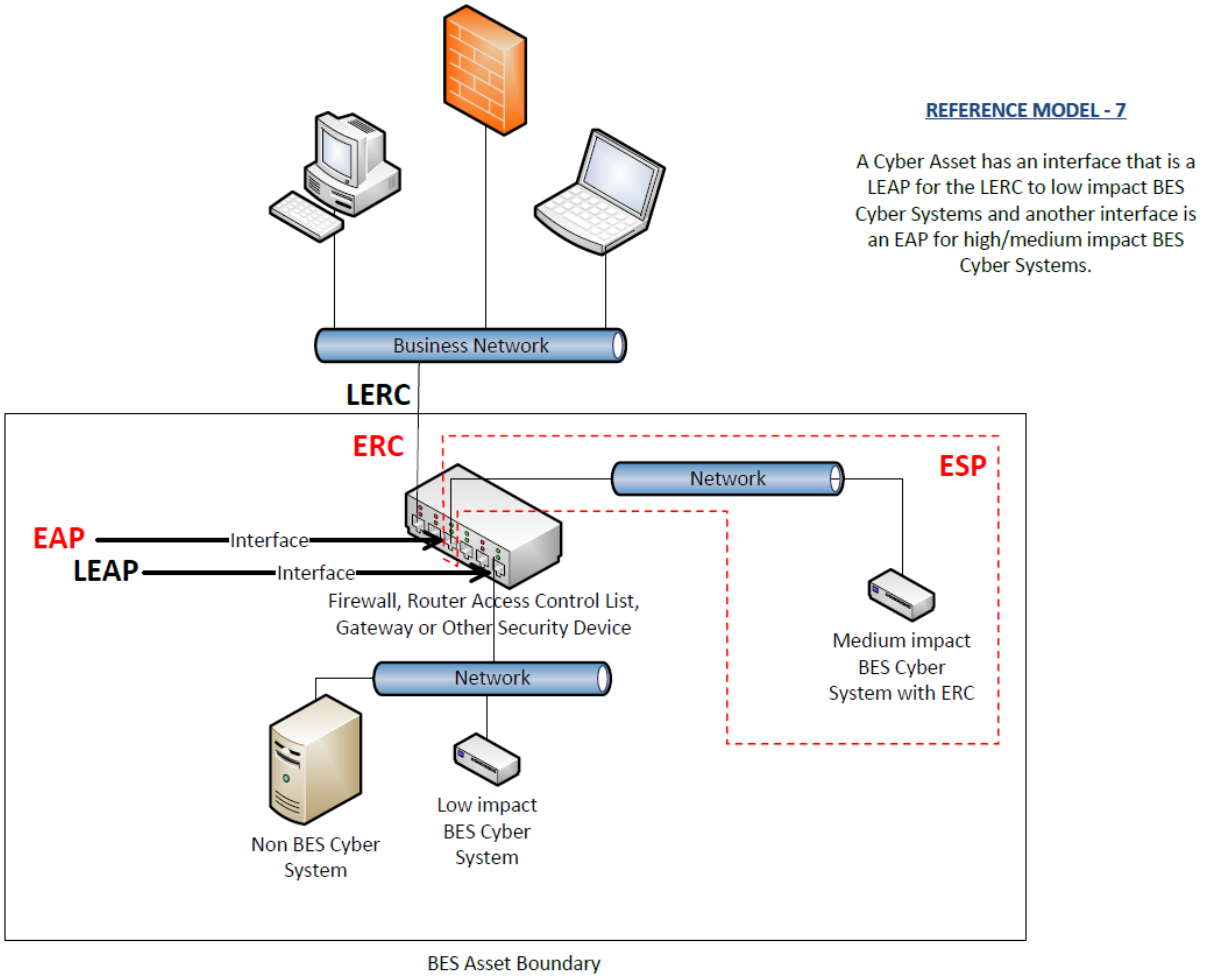
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

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

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-003-6 — Cyber Security - Security Management Controls

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-003-6	All	07/01/2016	

Printed On: May 12, 2016, 11:19 AM

CIP-004-6 Reliability Standard

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-6:

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-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-6.

6. Background:

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

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			locations, privileges were incorrect or unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR	termination action. (5.3)	date and time of the termination action. (5.3)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

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

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

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

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

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

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

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

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

Requirement R3:

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

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

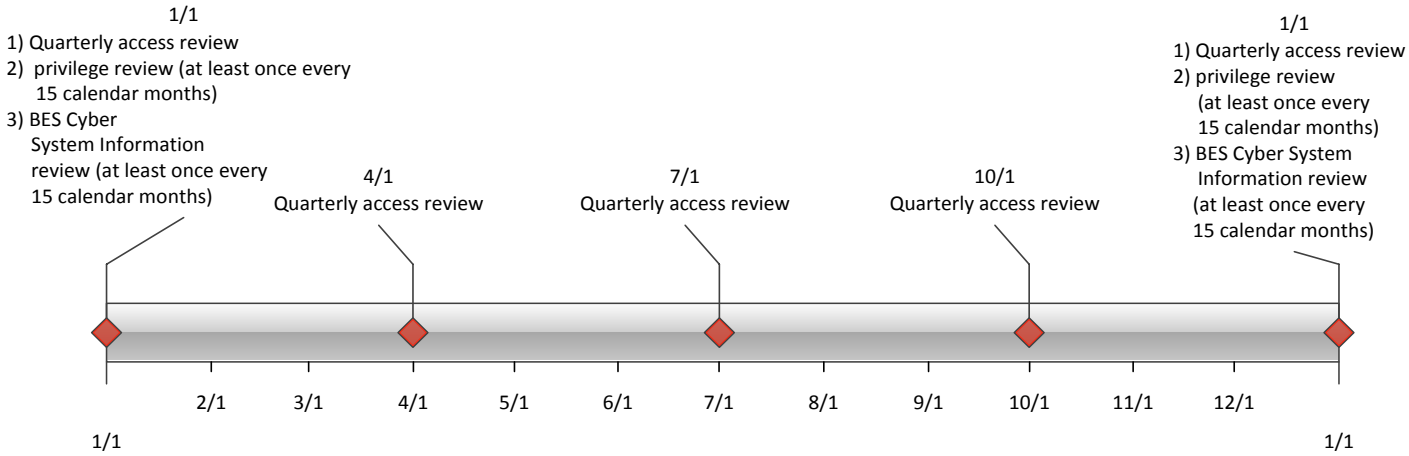
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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

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

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



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

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

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

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

Requirement R5:

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

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

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

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

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

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

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

Rationale:

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

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such

authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

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

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

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

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

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

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

Rationale for Requirement R5:

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

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

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

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-004-6 — Cyber Security - Personnel

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-004-6	All	07/01/2016	

Printed On: May 12, 2016, 11:19 AM

CIP-006-6 Reliability Standard

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems 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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

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-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable 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.
- **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.

- **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.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

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

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

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.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

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

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable

communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-006-6 — Cyber Security - Physical Security of BES Cyber Systems

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-006-6	All	07/01/2016	

Printed On: May 12, 2016, 11:19 AM

CIP-007-6 Reliability Standard

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

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

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

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-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-6.

6. Background:

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

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

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

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

B. Requirements and Measures

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

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

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

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

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

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

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

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

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

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

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

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

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

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

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

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

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

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

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

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

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

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

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

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

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

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

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

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

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

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

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.

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

Requirement R1:

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

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

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

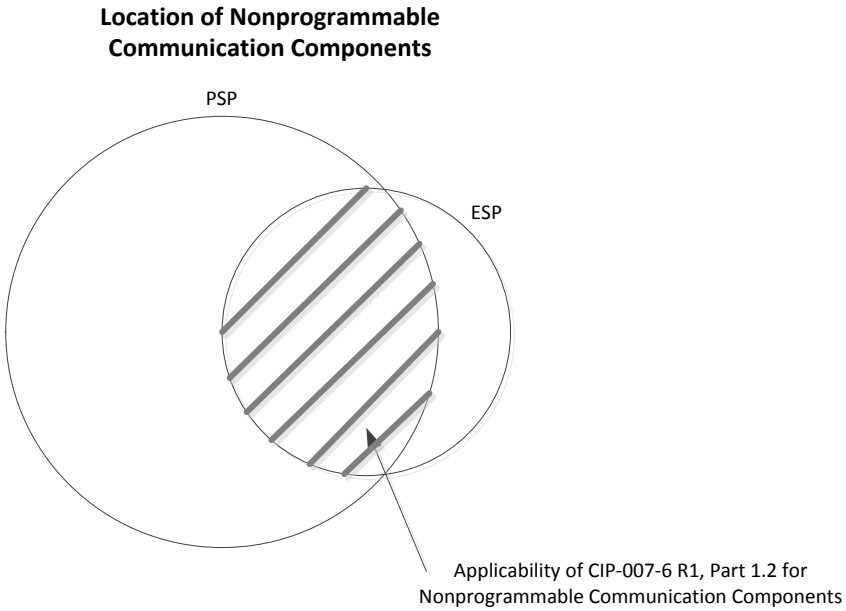
The protection of these ports can be accomplished in several ways including, but not limited to:

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

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

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

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



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

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

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

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

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

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

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

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

Requirement R3:

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

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

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

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

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

Requirement R4:

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

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

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

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

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

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

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

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

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

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

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

Requirement R5:

Account types referenced in this guidance typically include:

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

5.1 Reference the Requirement's rationale.

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

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

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

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

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

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

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

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

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

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

Rationale:

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

Rationale for Requirement R1:

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

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

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

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

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

Rationale for Requirement R5:

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

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

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

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

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

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

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

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

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

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

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-007-6 — Cyber Security - System Security Management

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-007-6	All	07/01/2016	

Printed On: May 12, 2016, 11:20 AM

CIP-009-6 Reliability Standard

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

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-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 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 their documented processes, but they 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and 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 include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

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

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

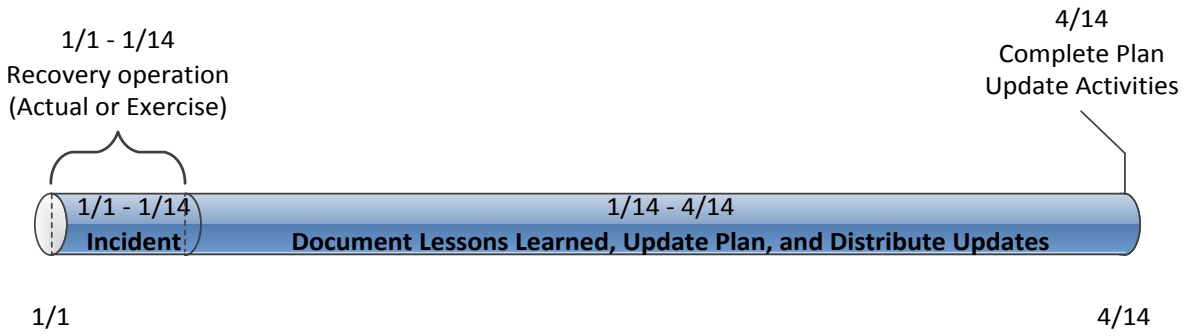


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

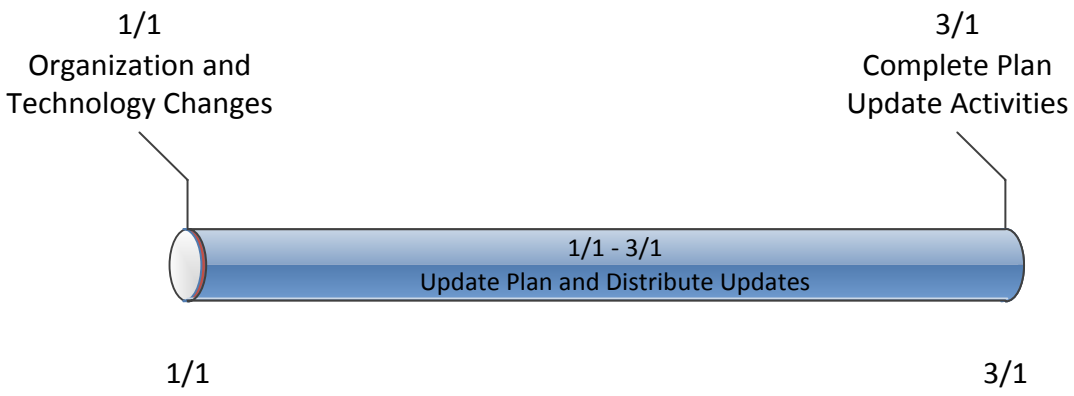


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

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

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-009-6 — Cyber Security - Recovery Plans for BES Cyber Systems

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-009-6	All	07/01/2016	

Printed On: May 12, 2016, 11:20 AM

CIP-010-2 Reliability Standard

A. Introduction

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

2. Number: CIP-010-2

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-2:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-010-2.

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-010-2 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-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 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-010-2 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-010-2 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-010-2 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.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 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-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 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-010-2 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-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 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-010-2 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-010-2 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:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	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)	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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						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 configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						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 #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	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	**Long-term Planning and Operations Planning**	**Medium**	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 15 months, but less than 18 months,	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 18 months, but less than 21, months	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 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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)	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)	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)	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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its 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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			manage its Transient Cyber Asset(s) according to CIP-010-2, 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 according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	implement the Removable Media sections according to CIP-010-2, 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 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	authorize its Transient Cyber Asset(s) according to CIP-010-2, 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 vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible	Removable Media according to CIP-010-2, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)	CIP-010-2, 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-010-2, Requirement R4, Attachment 1,	Entity according to CIP-010-2, 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-010-2, Requirement	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 2.1, 2.2, and 2.3. (R4)	R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-2. Docket No. RM15-14-000	

CIP-010-2 - 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-010-2 - 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).

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. 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.

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

- 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:

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

Rationale for Requirement R1:
The 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.

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-010-2 and CIP-007-6 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 ***

Enforcement Dates: Standard CIP-010-2 — Cyber Security - Configuration Change Management and Vulnerability Assessments

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-010-2	All	07/01/2016	

Printed On: May 12, 2016, 11:20 AM

CIP-011-2 Reliability Standard

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 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 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-2:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for CIP-011-2.

6. Background:

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

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

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

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

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

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

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

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

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

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

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

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

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

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

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

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

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

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

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

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

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

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

Requirement R2:

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

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

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

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

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

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

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

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

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

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

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

Rationale:

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

Rationale for Requirement R1:
The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard CIP-011-2 — Cyber Security - Information Protection

United States

Standard	Requirement	Enforcement Date	Inactive Date
CIP-011-2	All	07/01/2016	

Printed On: May 12, 2016, 11:20 AM

MOD-031-2 Reliability Standard

A. Introduction

1. Title: Demand and Energy Data

2. Number: MOD-031-2

3. Purpose: To provide authority for applicable entities to collect Demand, energy and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents of that data.

4. Applicability:

4.1. Functional Entities:

4.1.1 Planning Authority and Planning Coordinator (hereafter collectively referred to as the "Planning Coordinator")

This proposed standard combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria list "Planning Authority," and they are not yet synchronized. Until that occurs, the proposed standard applies to both "Planning Authority" and "Planning Coordinator."

4.1.2 Transmission Planner

4.1.3 Balancing Authority

4.1.4 Resource Planner

4.1.5 Load-Serving Entity

4.1.6 Distribution Provider

5. Effective Date

5.1. See the MOD-031-2 Implementation Plan.

6. Background:

To ensure that various forms of historical and forecast Demand and energy data and information is available to the parties that perform reliability studies and assessments, authority is needed to collect the applicable data.

The collection of Demand, Net Energy for Load and Demand Side Management data requires coordination and collaboration between Planning Authorities (Planning Coordinators), Transmission and Resource Planners, Load-Serving Entities and Distribution Providers. Ensuring that planners and operators have access to complete and accurate load forecasts – as well as the supporting methods and assumptions used to develop these forecasts – enhances the reliability of the Bulk Electric System. Consistent documenting and information sharing activities will also improve efficient planning practices and support the identification of needed system reinforcements. Furthermore, collection of actual Demand and Demand Side Management

performance during the prior year will allow for comparison to prior forecasts and further contribute to enhanced accuracy of load forecasting practices.

Data provided under this standard is generally considered confidential by Planning Coordinators and Balancing Authorities receiving the data. Furthermore, data reported to a Regional Entity is subject to the confidentiality provisions in Section 1500 of the North American Electric Reliability Corporation Rules of Procedure and is typically aggregated with data of other functional entities in a non-attributable manner. While this standard allows for the sharing of data necessary to perform certain reliability studies and assessments, any data received under this standard for which an applicable entity has made a claim of confidentiality should be maintained as confidential by the receiving entity.

B. Requirements and Measures

R1. Each Planning Coordinator or Balancing Authority that identifies a need for the collection of Total Internal Demand, Net Energy for Load, and Demand Side Management data shall develop and issue a data request to the applicable entities in its area. The data request shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. A list of Transmission Planners, Balancing Authorities, Load Serving Entities, and Distribution Providers that are required to provide the data ("Applicable Entities").

1.2. A timetable for providing the data. (A minimum of 30 calendar days must be allowed for responding to the request).

1.3. A request to provide any or all of the following actual data, as necessary:

1.3.1. Integrated hourly Demands in megawatts for the prior calendar year.

1.3.2. Monthly and annual integrated peak hour Demands in megawatts for the prior calendar year.

1.3.2.1. If the annual peak hour actual Demand varies due to weather-related conditions (e.g., temperature, humidity or wind speed), the Applicable Entity shall also provide the weather normalized annual peak hour actual Demand for the prior calendar year.

1.3.3. Monthly and annual Net Energy for Load in gigawatthours for the prior calendar year.

1.3.4. Monthly and annual peak hour controllable and dispatchable Demand Side Management under the control or supervision of the System Operator in megawatts for the prior calendar year. Three values shall be reported for each hour: 1) the committed megawatts (the amount under control or supervision), 2) the dispatched megawatts (the amount, if any,

activated for use by the System Operator), and 3) the realized megawatts (the amount of actual demand reduction).

1.4. A request to provide any or all of the following forecast data, as necessary:

1.4.1. Monthly peak hour forecast Total Internal Demands in megawatts for the next two calendar years.

1.4.2. Monthly forecast Net Energy for Load in gigawatthours for the next two calendar years.

1.4.3. Peak hour forecast Total Internal Demands (summer and winter) in megawatts for ten calendar years into the future.

1.4.4. Annual forecast Net Energy for Load in gigawatthours for ten calendar years into the future.

1.4.5. Total and available peak hour forecast of controllable and dispatchable Demand Side Management (summer and winter), in megawatts, under the control or supervision of the System Operator for ten calendar years into the future.

1.5. A request to provide any or all of the following summary explanations, as necessary,:

1.5.1. The assumptions and methods used in the development of aggregated Peak Demand and Net Energy for Load forecasts.

1.5.2. The Demand and energy effects of controllable and dispatchable Demand Side Management under the control or supervision of the System Operator.

1.5.3. How Demand Side Management is addressed in the forecasts of its Peak Demand and annual Net Energy for Load.

1.5.4. How the controllable and dispatchable Demand Side Management forecast compares to actual controllable and dispatchable Demand Side Management for the prior calendar year and, if applicable, how the assumptions and methods for future forecasts were adjusted.

1.5.5. How the peak Demand forecast compares to actual Demand for the prior calendar year with due regard to any relevant weather-related variations (e.g., temperature, humidity, or wind speed) and, if applicable, how the assumptions and methods for future forecasts were adjusted.

M1. The Planning Coordinator or Balancing Authority shall have a dated data request, either in hardcopy or electronic format, in accordance with Requirement R1.

R2. Each Applicable Entity identified in a data request shall provide the data requested by its Planning Coordinator or Balancing Authority in accordance with the data request issued pursuant to Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. Each Applicable Entity shall have evidence, such as dated e-mails or dated transmittal letters that it provided the requested data in accordance with Requirement R2.

R3. The Planning Coordinator or the Balancing Authority shall provide the data listed under Requirement R1 Parts 1.3 through 1.5 for their area to the applicable Regional Entity within 75 calendar days of receiving a request for such data, unless otherwise agreed upon by the parties. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M3. Each Planning Coordinator or Balancing Authority, shall have evidence, such as dated e-mails or dated transmittal letters that it provided the data requested by the applicable Regional Entity in accordance with Requirement R3.

R4. Any Applicable Entity shall, in response to a written request for the data included in parts 1.3-1.5 of Requirement R1 from a Planning Coordinator, Balancing Authority, Transmission Planner or Resource Planner with a demonstrated need for such data in order to conduct reliability assessments of the Bulk Electric System, provide or otherwise make available that data to the requesting entity. This requirement does not modify an entity's obligation pursuant to Requirement R2 to respond to data requests issued by its Planning Coordinator or Balancing Authority pursuant to Requirement R1. Unless otherwise agreed upon, the Applicable Entity: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- shall not be required to alter the format in which it maintains or uses the data;
- shall provide the requested data within 45 calendar days of the written request, subject to part 4.1 of this requirement; unless providing the requested data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements

4.1. If the Applicable Entity does not provide data requested because (1) the requesting entity did not demonstrate a reliability need for the data; or (2) providing the data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements, the Applicable Entity shall, within 30 calendar days of the written request, provide a written response to the requesting entity specifying the data that is not being provided and on what basis.

M4. Each Applicable Entity identified in Requirement R4 shall have evidence such as dated e-mails or dated transmittal letters that it provided the data requested or provided a written response specifying the data that is not being provided and the basis for not providing the data in accordance with Requirement R4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Evidence Retention

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

The Applicable Entity shall keep data or evidence to show compliance with Requirements R1 through R4, and Measures M1 through M4, since the last audit, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

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	Long-term Planning	Medium	N/A	N/A	N/A	The Planning Coordinator or Balancing Authority developed and issued a data request but failed to include either the entity(s) necessary to provide the data or the timetable for providing the data.
R2	Long-term Planning	Medium	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide all of the data requested in Requirement R1 part 1.5.1 through part 1.5.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide one of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide one of the requested items in Requirement R1 part	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide two of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide two of the requested items in Requirement R1 part	The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide three or more of the requested items in Requirement R1 part 1.3.1 through part 1.3.4 OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide three or more of the requested items in Requirement R1 part 1.4.1 through part 1.4.5

			did so after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 6 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	1.4.1 through part 1.4.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but did so 6 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 11 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	1.4.1 through part 1.4.5 OR The Applicable Entity, as defined in the data request developed in Requirement R1, provided the data requested in Requirement R1, but did so 11 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2 but prior to 15 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.	OR The Applicable Entity, as defined in the data request developed in Requirement R1, failed to provide the data requested in the timetable provided pursuant to Requirement R1 prior to 16 days after the date indicated in the timetable provided pursuant to Requirement R1 part 1.2.
R3	Long-term Planning	Medium	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 75 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 80 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, made available the data requested, but did so after 85 days	The Planning Coordinator or Balancing Authority, in response to a request by the Regional Entity, failed to make available the data requested prior to 91 days

			from the date of request but prior to 81 days from the date of the request.	from the date of request but prior to 86 days from the date of the request.	from the date of request but prior to 91 days from the date of the request.	or more from the date of the request.
R4	Long-term Planning	Medium	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 45 days from the date of request but prior to 51 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 30 days of the written request but prior to 36 days of the written resquest.	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 50 days from the date of request but prior to 56 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 35 days of the written request but prior to 41 days of the written resquest.	The Applicable Entity provided or otherwise made available the data to the requesting entity but did so after 55 days from the date of request but prior to 61 days from the date of the request OR The Applicable Entity that is not providing the data requested provided a written response specifying the data that is not being provided and on what basis but did so after 40 days of the written request but prior to 46 days of the written resquest.	The Applicable Entity failed to provide or otherwise make available the data to the requesting entity within 60 days from the date of the request OR The Applicable Entity that is not providing the data requested failed to provide a written response specifying the data that is not being provided and on what basis within 45 days of the written resquest.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 6, 2014	Adopted by the NERC Board of Trustees	
1	February 19, 2015	FERC order approving MOD-031-1	
2	November 5, 2015	Adopted by the NERC Board of Trustees	
2	February 18, 2016	FERC order approving MOD-031-2. Docket No. RD16-1-000	

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:

Rationale for R1: To ensure that when Planning Coordinators (PCs) or Balancing Authorities (BAs) request data (R1), they identify the entities that must provide the data (Applicable Entity in part 1.1), the data to be provided (parts 1.3 – 1.5) and the due dates (part 1.2) for the requested data.

For Requirement R1 part 1.3.2.1, if the Demand does not vary due to weather-related conditions (e.g., temperature, humidity or wind speed), or the weather assumed in the forecast was the same as the actual weather, the weather normalized actual Demand will be the same as the actual demand reported for Requirement R1 part 1.3.2. Otherwise the annual peak hour weather normalized actual Demand will be different from the actual demand reported for Requirement R1 part 1.3.2.

Balancing Authorities are included here to reflect a practice in the WECC Region where BAs are the entity that perform this requirement in lieu of the PC.

Rationale for R2:

This requirement will ensure that entities identified in Requirement R1, as responsible for providing data, provide the data in accordance with the details described in the data request developed in accordance with Requirement R1. In no event shall the Applicable Entity be required to provide data under this requirement that is outside the scope of parts 1.3 - 1.5 of Requirement R1.

Rationale for R3:

This requirement will ensure that the Planning Coordinator or when applicable, the Balancing Authority, provides the data requested by the Regional Entity.

Rationale for R4:

This requirement will ensure that the Applicable Entity will make the data requested by the Planning Coordinator or Balancing Authority in Requirement R1 available to other applicable entities (Planning Coordinator, Balancing Authority, Transmission Planner or Resource Planner) unless providing the data would conflict with the Applicable Entity's confidentiality, regulatory, or security requirements. The sharing of documentation of the supporting methods and assumptions used to develop forecasts as well as information-sharing activities will improve the efficiency of planning practices and support the identification of needed system reinforcements.

The obligation to share data under Requirement R4 does not supersede or otherwise modify any of the Applicable Entity's existing confidentiality obligations. For instance, if an entity is prohibited from providing any of the requested data pursuant to confidentiality provisions of an Open Access Transmission Tariff or a contractual arrangement, Requirement R4 does not

require the Applicable Entity to provide the data to a requesting entity. Rather, under Part 4.1, the Applicable Entity must simply provide written notification to the requesting entity that it will not be providing the data and the basis for not providing the data. If the Applicable Entity is subject to confidentiality obligations that allow the Applicable Entity to share the data only if certain conditions are met, the Applicable Entity shall ensure that those conditions are met within the 45-day time period provided in Requirement R4, communicate with the requesting entity regarding an extension of the 45-day time period so as to meet all those conditions, or provide justification under Part 4.1 as to why those conditions cannot be met under the circumstances.

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard MOD-031-2 — Demand and Energy Data

United States

Standard	Requirement	Enforcement Date	Inactive Date
MOD-031-2	All	10/01/2016	

Printed On: May 12, 2016, 11:11 AM

PRC-026-1 Reliability Standard

A. Introduction

1. **Title:** **Relay Performance During Stable Power Swings**

2. **Number:** **PRC-026-1**

3. **Purpose:** To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Generator Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.1.2 Planning Coordinator.

   4.1.3 Transmission Owner that applies load-responsive protective relays as described in PRC-026-1 – Attachment A at the terminals of the Elements listed in Section 4.2, Facilities.

   4.2. Facilities: The following Elements that are part of the Bulk Electric System (BES):

   4.2.1 Generators.

   4.2.2 Transformers.

   4.2.3 Transmission lines.

5. **Background:**

   This is the third phase of a three-phased standard development project that focused on developing this new Reliability Standard to address protective relay operations due to stable power swings. The March 18, 2010, Federal Energy Regulatory Commission (FERC) Order No. 733 approved Reliability Standard PRC-023-1 – Transmission Relay Loadability. In that Order, FERC directed NERC to address three areas of relay loadability that include modifications to the approved PRC-023-1, development of a new Reliability Standard to address generator protective relay loadability, and a new Reliability Standard to address the operation of protective relays due to stable power swings. This project's SAR addresses these directives with a three-phased approach to standard development.

   Phase 1 focused on making the specific modifications from FERC Order No. 733 to PRC-023-1. Reliability Standard PRC-023-2, which incorporated these modifications, became mandatory on July 1, 2012.

   Phase 2 focused on developing a new Reliability Standard, PRC-025-1 – Generator Relay Loadability, to address generator protective relay loadability. PRC-025-1 became mandatory on October 1, 2014, along with PRC-023-3, which was modified to harmonize PRC-023-2 with PRC-025-1.

   Phase 3 focuses on preventing protective relays from tripping unnecessarily due to stable power swings by requiring identification of Elements on which a stable or unstable power swing may affect Protection System operation, assessment of the security of load-

responsive protective relays to tripping in response to only a stable power swing, and implementation of Corrective Action Plans (CAP), where necessary. Phase 3 improves security of load-responsive protective relays for stable power swings so they are expected to not trip in response to stable power swings during non-Fault conditions while maintaining dependable fault detection and dependable out-of-step tripping.

6. Effective Dates:

Requirement R1

First day of the first full calendar year that is 12 months 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 full calendar year that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirements R2, R3, and R4

First day of the first full calendar year that is 36 months 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 full calendar year that is 36 months 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 Planning Coordinator shall, at least once each calendar year, provide notification of each generator, transformer, and transmission line BES Element in its area that meets one or more of the following criteria, if any, to the respective Generator Owner and Transmission Owner: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

Criteria:

1. Generator(s) where an angular stability constraint exists that is addressed by a System Operating Limit (SOL) or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s).
2. An Element that is monitored as part of an SOL identified by the Planning Coordinator's methodology[1] based on an angular stability constraint.
3. An Element that forms the boundary of an island in the most recent underfrequency load shedding (UFLS) design assessment based on application of the Planning Coordinator's criteria for identifying islands, only if the island is formed by tripping the Element due to angular instability.
4. An Element identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[2] power swing during a simulated disturbance.

M1. Each Planning Coordinator shall have dated evidence that demonstrates notification of the generator, transformer, and transmission line BES Element(s) that meet one or more of the criteria in Requirement R1, if any, to the respective Generator Owner and Transmission Owner. Evidence may include, but is not limited to, the following documentation: emails, facsimiles, records, reports, transmittals, lists, or spreadsheets.

[1] NERC Reliability Standard FAC-014-2 – Establish and Communicate System Operating Limits, Requirement R3.

[2] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

R2. Each Generator Owner and Transmission Owner shall: [Violation Risk Factor: High] [Time Horizon: Operations Planning]

2.1 Within 12 full calendar months of notification of a BES Element pursuant to Requirement R1, determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B where an evaluation of that Element's load-responsive protective relay(s) based on PRC-026-1 – Attachment B criteria has not been performed in the last five calendar years.

2.2 Within 12 full calendar months of becoming aware[3] of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable[4] power swing due to the operation of its protective relay(s), determine whether its load-responsive protective relay(s) applied to that BES Element meets the criteria in PRC-026-1 – Attachment B.

M2. Each Generator Owner and Transmission Owner shall have dated evidence that demonstrates the evaluation was performed according to Requirement R2. Evidence may include, but is not limited to, the following documentation: apparent impedance characteristic plots, email, design drawings, facsimiles, R-X plots, software output, records, reports, transmittals, lists, settings sheets, or spreadsheets.

R3. Each Generator Owner and Transmission Owner shall, within six full calendar months of determining a load-responsive protective relay does not meet the PRC-026-1 – Attachment B criteria pursuant to Requirement R2, develop a Corrective Action Plan (CAP) to meet one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- The Protection System meets the PRC-026-1 – Attachment B criteria, while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element); or
- The Protection System is excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element).

M3. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates the development of a CAP in accordance with Requirement R3. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

R4. Each Generator Owner and Transmission Owner shall implement each CAP developed pursuant to Requirement R3 and update each CAP if actions or timetables change until all actions are complete. *[Violation Risk Factor: Medium][Time Horizon: Long-Term Planning]*

M4. The Generator Owner and Transmission Owner shall have dated evidence that demonstrates implementation of each CAP according to Requirement R4, including updates to the CAP when actions or timetables change. Evidence may include, but is not limited to, the following documentation: corrective action plans, maintenance records, settings sheets, project or work management program records, or work orders.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Evidence Retention

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

The Generator Owner, Planning Coordinator, and Transmission Owner shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Planning Coordinator shall retain evidence of Requirement R1 for a minimum of one calendar year following the completion of the Requirement.
- The Generator Owner and Transmission Owner shall retain evidence of Requirement R2 evaluation for a minimum of 12 calendar months following completion of each evaluation where a CAP is not developed.
- The Generator Owner and Transmission Owner shall retain evidence of Requirements R2, R3, and R4 for a minimum of 12 calendar months following completion of each CAP.

If a Generator Owner, Planning Coordinator, or Transmission Owner 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.

[3] Some examples of the ways an entity may become aware of a power swing are provided in the Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing."

[4] An example of an unstable power swing is provided in the Guidelines and Technical Basis section, "Justification for Including Unstable Power Swings in the Requirements section of the Guidelines and Technical Basis."

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure; "Compliance Monitoring and 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	Long-term Planning	Medium	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was less than or equal to 30 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Planning Coordinator provided notification of the BES Element(s) in accordance with Requirement R1, but was more than 90 calendar days late. OR The Planning Coordinator failed to provide notification of the BES Element(s) in accordance with Requirement R1.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	High	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was less than or equal to 30 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 30 calendar days and less than or equal to 60 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 60 calendar days and less than or equal to 90 calendar days late.	The Generator Owner or Transmission Owner evaluated its load-responsive protective relay(s) in accordance with Requirement R2, but was more than 90 calendar days late. OR The Generator Owner or Transmission Owner failed to evaluate its load-responsive protective relay(s) in accordance with Requirement R2.

R#	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Long-term Planning	Medium	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than six calendar months and less than or equal to seven calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than seven calendar months and less than or equal to eight calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than eight calendar months and less than or equal to nine calendar months.	The Generator Owner or Transmission Owner developed a Corrective Action Plan (CAP) in accordance with Requirement R3, but in more than nine calendar months. OR The Generator Owner or Transmission Owner failed to develop a CAP in accordance with Requirement R3.
R4	Long-term Planning	Medium	The Generator Owner or Transmission Owner implemented a Corrective Action Plan (CAP), but failed to update a CAP when actions or timetables changed, in accordance with Requirement R4.	N/A	N/A	The Generator Owner or Transmission Owner failed to implement a Corrective Action Plan (CAP) in accordance with Requirement R4.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Applied Protective Relaying, Westinghouse Electric Corporation, 1979.

Burdy, John, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

IEEE Power System Relaying Committee WG D6, *Power Swing and Out-of-Step Considerations on Transmission Lines*, July 2005: http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Kimbark Edward Wilson, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

Kundur, Prabha, *Power System Stability and Control*, 1994, Palo Alto: EPRI, McGraw Hill, Inc.

NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf.

Reimert, Donald, *Protective Relaying for Power Generation Systems*, 2006, Boca Raton: CRC Press.

Version History

Version	Date	Action	Change Tracking
1	November 13, 2014	Adopted by NERC Board of Trustees	New
1	March 17, 2016	FERC Order issued approving PRC-026-1. Docket No. RM15-8-000.	

PRC-026-1 – Attachment A

This standard applies to any protective functions which could trip instantaneously or with a time delay of less than 15 cycles on load current (i.e., "load-responsive") including, but not limited to:

- Phase distance
- Phase overcurrent
- Out-of-step tripping
- Loss-of-field

The following protection functions are excluded from Requirements of this standard:

- Relay elements supervised by power swing blocking
- Relay elements that are only enabled when other relays or associated systems fail. For example:
    - Overcurrent elements that are only enabled during loss of potential conditions.
    - Relay elements that are only enabled during a loss of communications
- Thermal emulation relays which are used in conjunction with dynamic Facility Ratings
- Relay elements associated with direct current (dc) lines
- Relay elements associated with dc converter transformers
- Phase fault detector relay elements employed to supervise other load-responsive phase distance elements (i.e., in order to prevent false operation in the event of a loss of potential)
- Relay elements associated with switch-onto-fault schemes
- Reverse power relay on the generator
- Generator relay elements that are armed only when the generator is disconnected from the system, (e.g., non-directional overcurrent elements used in conjunction with inadvertent energization schemes, and open breaker flashover schemes)
- Current differential relay, pilot wire relay, and phase comparison relay
- Voltage-restrained or voltage-controlled overcurrent relays

PRC-026-1 – Attachment B

Criterion A:

An impedance-based relay used for tripping is expected to not trip for a stable power swing, when the relay characteristic is completely contained within the unstable power swing region.[5] The unstable power swing region is formed by the union of three shapes in the impedance (R-X) plane; (1) a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7; (2) an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43; (3) a lens that connects the endpoints of the total system impedance (with the parallel transfer impedance removed) bounded by varying the sending-end and receiving-end voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance where:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.

[5] Guidelines and Technical Basis, Figures 1 and 2.

PRC-026-1 – Attachment B

Criterion B:

The pickup of an overcurrent relay element used for tripping, that is above the calculated current value (with the parallel transfer impedance removed) for the conditions below:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
3. Saturated (transient or sub-transient) reactance is used for all machines.
4. Both the sending-end and receiving-end voltages at 1.05 per unit.

Guidelines and Technical Basis

Introduction

The NERC System Protection and Control Subcommittee technical document, *Protection System Response to Power Swings*, August 2013,[6] ("PSRPS Report" or "report") was specifically prepared to support the development of this NERC Reliability Standard. The report provided a historical perspective on power swings as early as 1965 up through the approval of the report by the NERC Planning Committee. The report also addresses reliability issues regarding trade-offs between security and dependability of Protection Systems, considerations for this NERC Reliability Standard, and a collection of technical information about power swing characteristics and varying issues with practical applications and approaches to power swings. Of these topics, the report suggests an approach for this NERC Reliability Standard ("standard" or "PRC-026-1") which is consistent with addressing three regulatory directives in the FERC Order No. 733. The first directive concerns the need for "…protective relay systems that differentiate between faults and stable power swings and, when necessary, phases out protective relay systems that cannot meet this requirement."[7] Second, is "…to develop a Reliability Standard addressing undesirable relay operation due to stable power swings."[8] The third directive "…to consider "islanding" strategies that achieve the fundamental performance for all islands in developing the new Reliability Standard addressing stable power swings"[9] was considered during development of the standard.

The development of this standard implements the majority of the approaches suggested by the report. However, it is noted that the Reliability Coordinator and Transmission Planner have not been included in the standard's Applicability section (as suggested by the PSRPS Report). This is so that a single entity, the Planning Coordinator, may be the single source for identifying Elements according to Requirement R1. A single source will insure that multiple entities will not identify Elements in duplicate, nor will one entity fail to provide an Element because it believes the Element is being provided by another entity. The Planning Coordinator has, or has access to, the wide-area model and can correctly identify the Elements that may be susceptible to a stable or unstable power swing. Additionally, not including the Reliability Coordinator and Transmission Planner is consistent with the applicability of other relay loadability NERC Reliability Standards (e.g., PRC-023 and PRC-025). It is also consistent with the NERC Functional Model.

The phrase, "while maintaining dependable fault detection and dependable out-of-step tripping" in Requirement R3, describes that the Generator Owner and Transmission Owner are to comply with this standard while achieving its desired protection goals. Load-responsive protective relays, as addressed within this standard, may be intended to provide a variety of backup protection functions, both within the generating unit or generating plant and on the transmission system, and

---

[6] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

[7] Transmission Relay Loadability Reliability Standard, Order No. 733, P.150 FERC ¶ 61,221 (2010).

[8] Ibid. P.153.

[9] Ibid. P.162.

this standard is not intended to result in the loss of these protection functions. Instead, the Generator Owner and Transmission Owner must consider both the Requirements within this standard and its desired protection goals and perform modifications to its protective relays or protection philosophies as necessary to achieve both.

Power Swings

The IEEE Power System Relaying Committee WG D6 developed a technical document called *Power Swing and Out-of-Step Considerations on Transmission Lines* (July 2005) that provides background on power swings. The following are general definitions from that document:[10]

> Power Swing: a variation in three phase power flow which occurs when the generator rotor angles are advancing or retarding relative to each other in response to changes in load magnitude and direction, line switching, loss of generation, faults, and other system disturbances.
>
> Pole Slip: a condition whereby a generator, or group of generators, terminal voltage angles (or phases) go past 180 degrees with respect to the rest of the connected power system.
>
> Stable Power Swing: a power swing is considered stable if the generators do not slip poles and the system reaches a new state of equilibrium, i.e. an acceptable operating condition.
>
> Unstable Power Swing: a power swing that will result in a generator or group of generators experiencing pole slipping for which some corrective action must be taken.
>
> Out-of-Step Condition: Same as an unstable power swing.
>
> Electrical System Center or Voltage Zero: it is the point or points in the system where the voltage becomes zero during an unstable power swing.

Burden to Entities

The PSRPS Report provides a technical basis and approach for focusing on Protection Systems, which are susceptible to power swings, while achieving the purpose of the standard. The approach reduces the number of relays to which the PRC-026-1 Requirements would apply by first identifying the BES Element(s) on which load-responsive protective relays must be evaluated. The first step uses criteria to identify the Elements on which a Protection System is expected to be challenged by power swings. Of those Elements, the second step is to evaluate each load-responsive protective relay that is applied on each identified Element. Rather than requiring the Planning Coordinator or Transmission Planner to perform simulations to obtain information for each identified Element, the Generator Owner and Transmission Owner will reduce the need for simulation by comparing the load-responsive protective relay characteristic to specific criteria in PRC-026-1 – Attachment B.

[10] http://www.pes-psrc.org/Reports/Power%20Swing%20and%20OOS%20Considerations%20on%20Transmission%20Lines%20F..pdf.

Applicability

The standard is applicable to the Generator Owner, Planning Coordinator, and Transmission Owner entities. More specifically, the Generator Owner and Transmission Owner entities are applicable when applying load-responsive protective relays at the terminals of the applicable BES Elements. The standard is applicable to the following BES Elements: generators, transformers, and transmission lines. The Distribution Provider was considered for inclusion in the standard; however, it is not subject to the standard because this entity, by functional registration, would not own generators, transmission lines, or transformers other than load serving.

Load-responsive protective relays include any protective functions which could trip with or without time delay, on load current.

Requirement R1

The Planning Coordinator has a wide-area view and is in the position to identify what, if any, Elements meet the criteria. The criterion-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document, *Protection System Response to Power Swings (*August 2013),[11] which recommends a focused approach to determine an at-risk Element. Identification of Elements comes from the annual Planning Assessments pursuant to the transmission planning (i.e., "TPL") and other NERC Reliability Standards (e.g., PRC-006), and the standard is not requiring any other assessments to be performed by the Planning Coordinator. The required notification on a calendar year basis to the respective Generator Owner and Transmission Owner is sufficient because it is expected that the Planning Coordinator will make its notifications following the completion of its annual Planning Assessments. The Planning Coordinator will continue to provide notification of Elements on a calendar year basis even if a study is performed less frequently (e.g., PRC-006 – Automatic Underfrequency Load Shedding, which is five years) and has not changed. It is possible that a Planning Coordinator could utilize studies from a prior year in determining the necessary notifications pursuant to Requirement R1.

Criterion 1

The first criterion involves generator(s) where an angular stability constraint exists that is addressed by a System Operating Limit (SOL) or a Remedial Action Scheme (RAS) and those Elements terminating at the Transmission station associated with the generator(s). For example, a scheme to remove generation for specific conditions is implemented for a four-unit generating plant (1,100 MW). Two of the units are 500 MW each; one is connected to the 345 kV system and one is connected to the 230 kV system. The Transmission Owner has two 230 kV transmission lines and one 345 kV transmission line all terminating at the generating facility as well as a 345/230 kV autotransformer. The remaining 100 MW consists of two 50 MW combustion turbine (CT) units connected to four 66 kV transmission lines. The 66 kV transmission lines are not electrically joined to the 345 kV and 230 kV transmission lines at the plant site and are not subject to the operating limit or RAS. A stability constraint limits the output of the portion of the plant affected

[11] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20 20/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

by the RAS to 700 MW for an outage of the 345 kV transmission line. The RAS trips one of the 500 MW units to maintain stability for a loss of the 345 kV transmission line when the total output from both 500 MW units is above 700 MW. For this example, both 500 MW generating units and the associated generator step-up (GSU) transformers would be identified as Elements meeting this criterion. The 345/230 kV autotransformer, the 345 kV transmission line, and the two 230 kV transmission lines would also be identified as Elements meeting this criterion. The 50 MW combustion turbines and 66 kV transmission lines would not be identified pursuant to Criterion 1 because these Elements are not subject to an operating limit or RAS and do not terminate at the Transmission station associated with the generators that are subject to the SOL or RAS.

Criterion 2

The second criterion involves Elements that are monitored as a part of an established System Operating Limit (SOL) based on an angular stability limit regardless of the outage conditions that result in the enforcement of the SOL. For example, if two long parallel 500 kV transmission lines have a combined SOL of 1,200 MW, and this limit is based on angular instability resulting from a fault and subsequent loss of one of the two lines, then both lines would be identified as Elements meeting the criterion.

Criterion 3

The third criterion involves Elements that form the boundary of an island within an underfrequency load shedding (UFLS) design assessment. The criterion applies to islands identified based on application of the Planning Coordinator's criteria for identifying islands, where the island is formed by tripping the Elements based on angular instability. The criterion applies if the angular instability is modeled in the UFLS design assessment, or if the boundary is identified "off-line" (i.e., the Elements are selected based on angular instability considerations, but the Elements are tripped in the UFLS design assessment without modeling the initiating angular instability). In cases where an out-of-step condition is detected and tripping is initiated at an alternate location, the criterion applies to the Element on which the power swing is detected. The criterion does not apply to islands identified based on other considerations that do not involve angular instability, such as excessive loading, Planning Coordinator area boundary tie lines, or Balancing Authority boundary tie lines.

Criterion 4

The fourth criterion involves Elements identified in the most recent annual Planning Assessment where relay tripping occurs due to a stable or unstable[12] power swing during a simulated disturbance. The intent is for the Planning Coordinator to include any Element(s) where relay tripping was observed during simulations performed for the most recent annual Planning Assessment associated with the transmission planning TPL-001-4 Reliability Standard. Note that relay tripping must be assessed within those annual Planning Assessments per TPL-001-4, R4,

[12] Refer to the "Justification for Including Unstable Power Swings in the Requirements" section.

Part 4.3.1.3, which indicates that analysis shall include the "Tripping of Transmission lines and transformers where transient swings cause Protection System operation based on generic or actual relay models." Identifying such Elements according to Criterion 4 and notifying the respective Generator Owner and Transmission Owner will require that the owners of any load-responsive protective relay applied at the terminals of the identified Element evaluate the relay's susceptibility to tripping in response to a stable power swing.

Planning Coordinators have the discretion to determine whether the observed tripping for a power swing in its Planning Assessments occurs for valid contingencies and system conditions. The Planning Coordinator will address tripping that is observed in transient analyses on an individual basis; therefore, the Planning Coordinator is responsible for identifying the Elements based only on simulation results that are determined to be valid.

Due to the nature of how a Planning Assessment is performed, there may be cases where a previously-identified Element is not identified in the most recent annual Planning Assessment. If so, this is acceptable because the Generator Owner and Transmission Owner would have taken action upon the initial notification of the previously identified Element. When an Element is not identified in later Planning Assessments, the risk of load-responsive protective relays tripping in response to a stable power swing during non-Fault conditions would have already been assessed under Requirement R2 and mitigated according to Requirements R3 and R4 where the relays did not meet the PRC-026-1 – Attachment B criteria. According to Requirement R2, the Generator Owner and Transmission Owner are only required to re-evaluate each load-responsive protective relay for an identified Element where the evaluation has not been performed in the last five calendar years.

Although Requirement R1 requires the Planning Coordinator to notify the respective Generator Owner and Transmission Owner of any Elements meeting one or more of the four criteria, it does not preclude the Planning Coordinator from providing additional information, such as apparent impedance characteristics, in advance or upon request, that may be useful in evaluating protective relays. Generator Owners and Transmission Owners are able to complete protective relay evaluations and perform the required actions without additional information. The standard does not include any requirement for the entities to provide information that is already being shared or exchanged between entities for operating needs. While a Requirement has not been included for the exchange of information, entities should recognize that relay performance needs to be measured against the most current information.

Requirement R2

Requirement R2 requires the Generator Owner and Transmission Owner to evaluate its load-responsive protective relays to ensure that they are expected to not trip in response to stable power swings.

The PRC-026-1 – Attachment A lists the applicable load-responsive relays that must be evaluated which include phase distance, phase overcurrent, out-of-step tripping, and loss-of-field relay functions. Phase distance relays could include, but are not limited to, the following:

- Zone elements with instantaneous tripping or intentional time delays of less than 15 cycles
- Phase distance elements used in high-speed communication-aided tripping schemes including:
  - Directional Comparison Blocking (DCB) schemes
  - Directional Comparison Un-Blocking (DCUB) schemes
  - Permissive Overreach Transfer Trip (POTT) schemes
  - Permissive Underreach Transfer Trip (PUTT) schemes

A method is provided within the standard to support consistent evaluation by Generator Owners and Transmission Owners based on specified conditions. Once a Generator Owner or Transmission Owner is notified of Elements pursuant to Requirement R1, it has 12 full calendar months to determine if each Element's load-responsive protective relays meet the PRC-026-1 – Attachment B criteria, if the determination has not been performed in the last five calendar years. Additionally, each Generator Owner and Transmission Owner, that becomes aware of a generator, transformer, or transmission line BES Element that tripped in response to a stable or unstable power swing due to the operation of its protective relays pursuant to Requirement R2, Part 2.2, must perform the same PRC-026-1 – Attachment B criteria determination within 12 full calendar months.

Becoming Aware of an Element That Tripped in Response to a Power Swing

Part 2.2 in Requirement R2 is intended to initiate action by the Generator Owner and Transmission Owner when there is a known stable or unstable power swing and it resulted in the entity's Element tripping. The criterion starts with becoming aware of the event (i.e., power swing) and then any connection with the entity's Element tripping. By doing so, the focus is removed from the entity having to demonstrate that it made a determination whether a power swing was present for every Element trip. The basis for structuring the criterion in this manner is driven by the available ways that a Generator Owner and Transmission Owner could become aware of an Element that tripped in response to a stable or unstable power swing due to the operation of its protective relay(s).

Element trips caused by stable or unstable power swings, though infrequent, would be more common in a larger event. The identification of power swings will be revealed during an analysis of the event. Event analysis where an entity may become aware of a stable or unstable power swing could include internal analysis conducted by the entity, the entity's Protection System review following a trip, or a larger scale analysis by other entities. Event analysis could include involvement by the entity's Regional Entity, and in some cases NERC.

Information Common to Both Generation and Transmission Elements

The PRC-026-1 – Attachment A lists the load-responsive protective relays that are subject to this standard. Generator Owners and Transmission Owners may own load-responsive protective relays (e.g., distance relays) that directly affect generation or transmission BES Elements and will require analysis as a result of Elements being identified by the Planning Coordinator in Requirement R1

or the Generator Owner or Transmission Owner in Requirement R2. For example, distance relays owned by the Transmission Owner may be installed at the high-voltage side of the generator step-up (GSU) transformer (directional toward the generator) providing backup to generation protection. Generator Owners may have distance relays applied to backup transmission protection or backup protection to the GSU transformer. The Generator Owner may have relays installed at the generator terminals or the high-voltage side of the GSU transformer.

Exclusion of Time Based Load-Responsive Protective Relays

The purpose of the standard is "[t]o ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions." Load-responsive, high-speed tripping protective relays pose the highest risk of operating during a power swing. Because of this, high-speed tripping protective relays and relays with a time delay of less than 15 cycles are included in the standard; whereas other relays (i.e., Zones 2 and 3) with a time delay of 15 cycles or greater are excluded. The time delay used for exclusion on some load-responsive protective relays is based on the maximum expected time that load-responsive protective relays would be exposed to a stable power swing with a slow slip rate frequency.

In order to establish a time delay that distinguishes a high-risk load-responsive protective relay from one that has a time delay for tripping (lower-risk), a sample of swing rates were calculated based on a stable power swing entering and leaving the impedance characteristic as shown in Table 1. For a relay impedance characteristic that has a power swing entering and leaving, beginning at 90 degrees with a termination at 120 degrees before exiting the zone, the zone timer must be greater than the calculated time the stable power swing is inside the relay's operating zone to not trip in response to the stable power swing.

Eq. (1)
$$Zone\ timer > 2 \times \left(\frac{(120° - Angle\ of\ entry\ into\ the\ relay\ characteristic) \times 60}{(360 \times Slip\ Rate)}\right)$$

Table 1: Swing Rates

Zone Timer (Cycles)	Slip Rate (Hz)
10	1.00
15	0.67
20	0.50
30	0.33

With a minimum zone timer of 15 cycles, the corresponding slip rate of the system is 0.67 Hz. This represents an approximation of a slow slip rate during a system Disturbance. Longer time delays allow for slower slip rates.

Application to Transmission Elements

Criterion A in PRC-026-1 – Attachment B describes an unstable power swing region that is formed by the union of three shapes in the impedance (R-X) plane. The first shape is a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7 (i.e., E_S / E_R = 0.7 / 1.0 = 0.7). The second shape is an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43 (i.e., E_S / E_R = 1.0 / 0.7 = 1.43). The third shape is a lens that connects the endpoints of the total system impedance together by varying the sending-end and receiving-end system voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance (with the parallel transfer impedance removed—see Figures 1 through 5). The total system impedance is derived from a two-bus equivalent network and is determined by summing the sending-end source impedance, the line impedance (excluding the Thévenin equivalent transfer impedance), and the receiving-end source impedance as shown in Figures 6 and 7. Establishing the total system impedance provides a conservative condition that will maximize the security of the relay against various system conditions. The smallest total system impedance represents a condition where the size of the lens characteristic in the R-X plane is smallest and is a conservative operating point from the standpoint of ensuring a load-responsive protective relay is expected to not trip given a predetermined angular displacement between the sending-end and receiving-end voltages. The smallest total system impedance results when all generation is in service and all transmission BES Elements are modeled in their "normal" system configuration (PRC-026-1 – Attachment B, Criterion A). The parallel transfer impedance is removed to represent a likely condition where parallel Elements may be lost during the disturbance, and the loss of these Elements magnifies the sensitivity of the load-responsive relays on the parallel line by removing the "infeed effect" (i.e., the apparent impedance sensed by the relay is decreased as a result of the loss of the transfer impedance, thus making the relay more likely to trip for a stable power swing—See Figures 13 and 14).

The sending-end and receiving-end source voltages are varied from 0.7 to 1.0 per unit to form the lower and upper loss-of-synchronism circles. The ratio of these two voltages is used in the calculation of the loss-of-synchronism circles, and result in a ratio range from 0.7 to 1.43.

Eq. (2) $$\frac{E_S}{E_R} = \frac{0.7}{1.0} = 0.7$$

Eq. (3): $$\frac{E_S}{E_R} = \frac{1.0}{0.7} = 1.43$$

The internal generator voltage during severe power swings or transmission system fault conditions will be greater than zero due to voltage regulator support. The voltage ratio of 0.7 to 1.43 is chosen to be more conservative than the PRC-023[13] and PRC-025[14] NERC Reliability Standards where a lower bound voltage of 0.85 per unit voltage is used. A ±15% internal generator voltage range was chosen as a conservative voltage range for calculation of the voltage ratio used to calculate the loss-of-synchronism circles. For example, the voltage ratio using these voltages would result in a ratio range from 0.739 to 1.353.

[13] Transmission Relay Loadability

[14] Generator Relay Loadability

Eq. (4) $$\frac{E_S}{E_R} = \frac{0.85}{1.15} = 0.739$$ Eq. (5): $$\frac{E_S}{E_R} = \frac{1.15}{0.85} = 1.353$$

The lower ratio is rounded down to 0.7 to be more conservative, allowing a voltage range of 0.7 to 1.0 per unit to be used for the calculation of the loss-of-synchronism circles.[15]

When the parallel transfer impedance is included in the model, the division of current through the parallel transfer impedance path results in actual measured relay impedances that are larger than those measured when the parallel transfer impedance is removed (i.e., infeed effect), which would make it more likely for an impedance relay element to be completely contained within the unstable power swing region as shown in Figure 11. If the transfer impedance is included in the evaluation, a distance relay element could be deemed as meeting PRC-026-1 – Attachment B criteria and, in fact would be secure, assuming all Elements were in their normal state. In this case, the distance relay element could trip in response to a stable power swing during an actual event if the system was weakened (i.e., a higher transfer impedance) by the loss of a subset of lines that make up the parallel transfer impedance as shown in Figure 10. This could happen because the subset of lines that make up the parallel transfer impedance tripped on unstable swings, contained the initiating fault, and/or were lost due to operation of breaker failure or remote back-up protection schemes.

Table 10 shows the percent size increase of the lens shape as seen by the relay under evaluation when the parallel transfer impedance is included. The parallel transfer impedance has minimal effect on the apparent size of the lens shape as long as the parallel transfer impedance is at least 10 multiples of the parallel line impedance (less than 5% lens shape expansion), therefore, its removal has minimal impact, but results in a slightly more conservative, smaller lens shape. Parallel transfer impedances of 5 multiples of the parallel line impedance or less result in an apparent lens shape size of 10% or greater as seen by the relay. If two parallel lines and a parallel transfer impedance tie the sending-end and receiving-end buses together, the total parallel transfer impedance will be one or less multiples of the parallel line impedance, resulting in an apparent lens shape size of 45% or greater. It is a realistic contingency that the parallel line could be out-of-service, leaving the parallel transfer impedance making up the rest of the system in parallel with the line impedance. Since it is not known exactly which lines making up the parallel transfer impedance will be out of service during a major system disturbance, it is most conservative to assume that all of them are out, leaving just the line under evaluation in service.

Either the saturated transient or sub-transient direct axis reactance may be used for machines in the evaluation because they are smaller than the un-saturated reactances. Since saturated sub-transient generator reactances are smaller than the transient or synchronous reactances, the use of sub-transient reactances will result in a smaller source impedance and a smaller unstable power swing region in the graphical analysis as shown in Figures 8 and 9. Because power swings occur in a time frame where generator transient reactances will be prevalent, it is acceptable to use saturated transient reactances instead of saturated sub-transient reactances. Because some short-

[15] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Section 6 (The Cascade Stage of the Blackout), p. 94 under "Why the Generators Tripped Off," states, "Some generator undervoltage relays were set to trip at or above 90% voltage. However, a motor stalls out at about 70% voltage and a motor starter contactor drops out around 75%, so if there is a compelling need to protect the turbine from the system the under-voltage trigger point should be no higher than 80%."

circuit models may not include transient reactances, the use of sub-transient reactances is also acceptable because it produces more conservative results. For this reason, either value is acceptable when determining the system source impedances (PRC-026-1 – Attachment B, Criterion A and B, No. 3).

Saturated reactances are used in short-circuit programs that produce the system impedance mentioned above. Planning and stability software generally use un-saturated reactances. Generator models used in transient stability analyses recognize that the extent of the saturation effect depends upon both rotor (field) and stator currents. Accordingly, they derive the effective saturated parameters of the machine at each instant by internal calculation from the specified (constant) unsaturated values of machine reactances and the instantaneous internal flux level. The specific assumptions regarding which inductances are affected by saturation, and the relative effect of that saturation, are different for the various generator models used. Thus, unsaturated values of all machine reactances are used in setting up planning and stability software data, and the appropriate set of open-circuit magnetization curve data is provided for each machine.

Saturated reactance values are smaller than unsaturated reactance values and are used in short-circuit programs owned by the Generator and Transmission Owners. Because of this, saturated reactance values are to be used in the development of the system source impedances.

The source or system equivalent impedances can be obtained by a number of different methods using commercially available short-circuit calculation tools.[16] Most short-circuit tools have a network reduction feature that allows the user to select the local and remote terminal buses to retain. The first method reduces the system to one that contains two buses, an equivalent generator at each bus (representing the source impedances at the sending-end and receiving-end), and two parallel lines; one being the line impedance of the protected line with relays being analyzed, the other being the parallel transfer impedance representing all other combinations of lines that connect the two buses together as shown in Figure 6. Another conservative method is to open both ends of the line being evaluated, and apply a three-phase bolted fault at each bus to determine the Thévenin equivalent impedance at each bus. The source impedances are set equal to the Thévenin equivalent impedances and will be less than or equal to the actual source impedances calculated by the network reduction method. Either method can be used to develop the system source impedances at both ends.

The two bullets of PRC-026-1 – Attachment B, Criterion A, No. 1, identify the system separation angles used to identify the size of the power swing stability boundary for evaluating load-responsive protective relay impedance elements. The first bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates a system separation angle of at least 120 degrees that is held constant while varying the sending-end and receiving-end source voltages from 0.7 to 1.0 per unit, thus creating an unstable power swing region about the total system impedance in Figure 1. This unstable power swing region is compared to the tripping portion of the distance relay characteristic; that is, the portion that is not supervised by load encroachment, blinders, or some other form of supervision as shown in Figure 12 that restricts the distance element from tripping

[16] Demetrios A. Tziouvaras and Daqing Hou, Appendix in *Out-Of-Step Protection Fundamentals and Advancements,* April 17, 2014: https://www.selinc.com.

for heavy, balanced load conditions. If the tripping portion of the impedance characteristics are completely contained within the unstable power swing region, the relay impedance element meets Criterion A in PRC-026-1 – Attachment B. A system separation angle of 120 degrees was chosen for the evaluation because it is generally accepted in the industry that recovery for a swing beyond this angle is unlikely to occur.[17]

The second bullet of PRC-026-1 – Attachment B, Criterion A, No. 1 evaluates impedance relay elements at a system separation angle of less than 120 degrees, similar to the first bullet described above. An angle less than 120 degrees may be used if a documented stability analysis demonstrates that the power swing becomes unstable at a system separation angle of less than 120 degrees.

The exclusion of relay elements supervised by Power Swing Blocking (PSB) in PRC-026-1 – Attachment A allows the Generator Owner or Transmission Owner to exclude protective relay elements if they are blocked from tripping by PSB relays. A PSB relay applied and set according to industry accepted practices prevent supervised load-responsive protective relays from tripping in response to power swings. Further, PSB relays are set to allow dependable tripping of supervised elements. The criteria in PRC-026-1 – Attachment B specifically applies to unsupervised elements that could trip for stable power swings. Therefore, load-responsive protective relay elements supervised by PSB can be excluded from the Requirements of this standard.

[17] "The critical angle for maintaining stability will vary depending on the contingency and the system condition at the time the contingency occurs; however, the likelihood of recovering from a swing that exceeds 120 degrees is marginal and 120 degrees is generally accepted as an appropriate basis for setting out-of-step protection. Given the importance of separating unstable systems, defining 120 degrees as the critical angle is appropriate to achieve a proper balance between dependable tripping for unstable power swings and secure operation for stable power swings." NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf), p. 28.

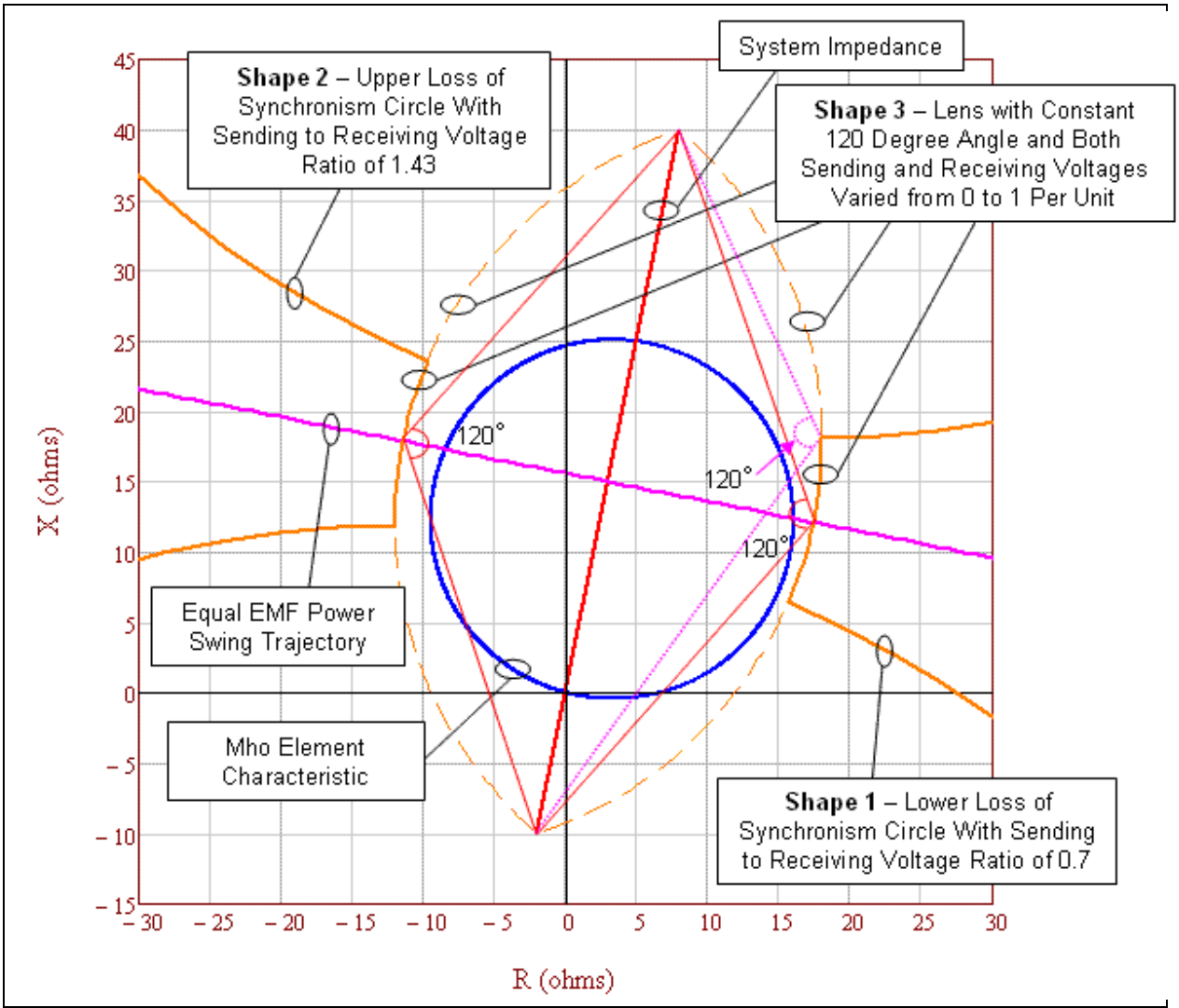


Figure 1: An enlarged graphic illustrating the unstable power swing region formed by the union of three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region (i.e., it does not intersect any portion of the unstable power swing region), therefore it meets PRC-026-1 – Attachment B, Criterion A, No. 1.

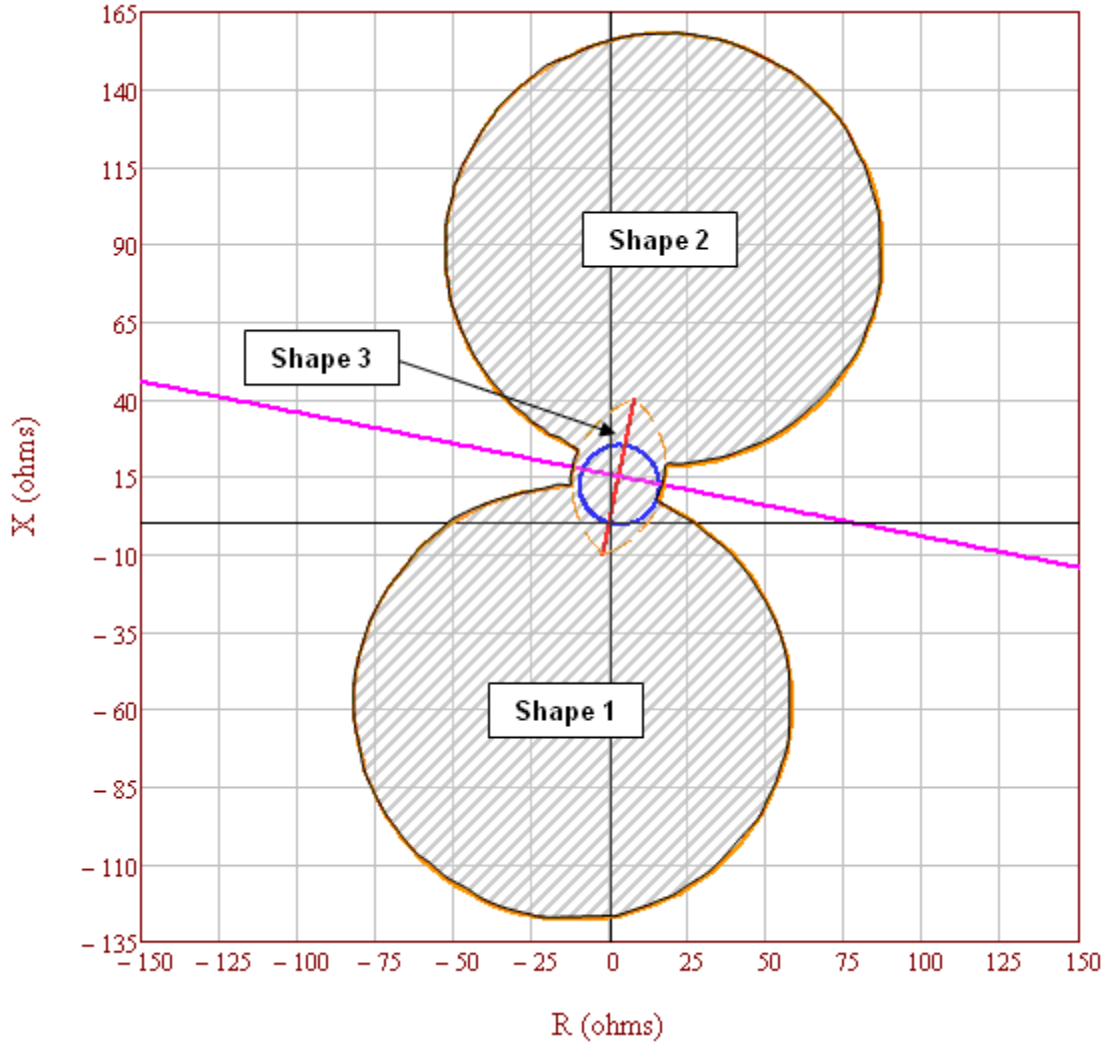


Figure 2: Full graphic of the unstable power swing region formed by the union of the three shapes in the impedance (R-X) plane: Shape 1) Lower loss-of-synchronism circle, Shape 2) Upper loss-of-synchronism circle, and Shape 3) Lens. The mho element characteristic is completely contained within the unstable power swing region, therefore it meets PRC-26-1 – Attachment B, Criterion A, No.1.

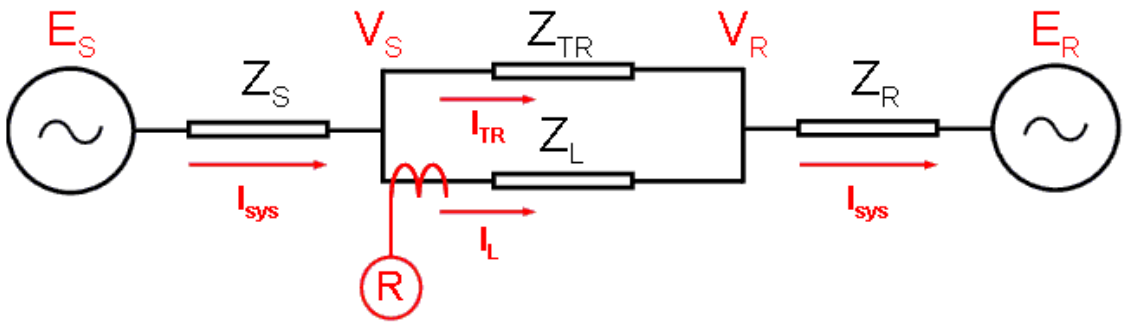


Figure 3: System impedances as seen by Relay R (voltage connections are not shown).

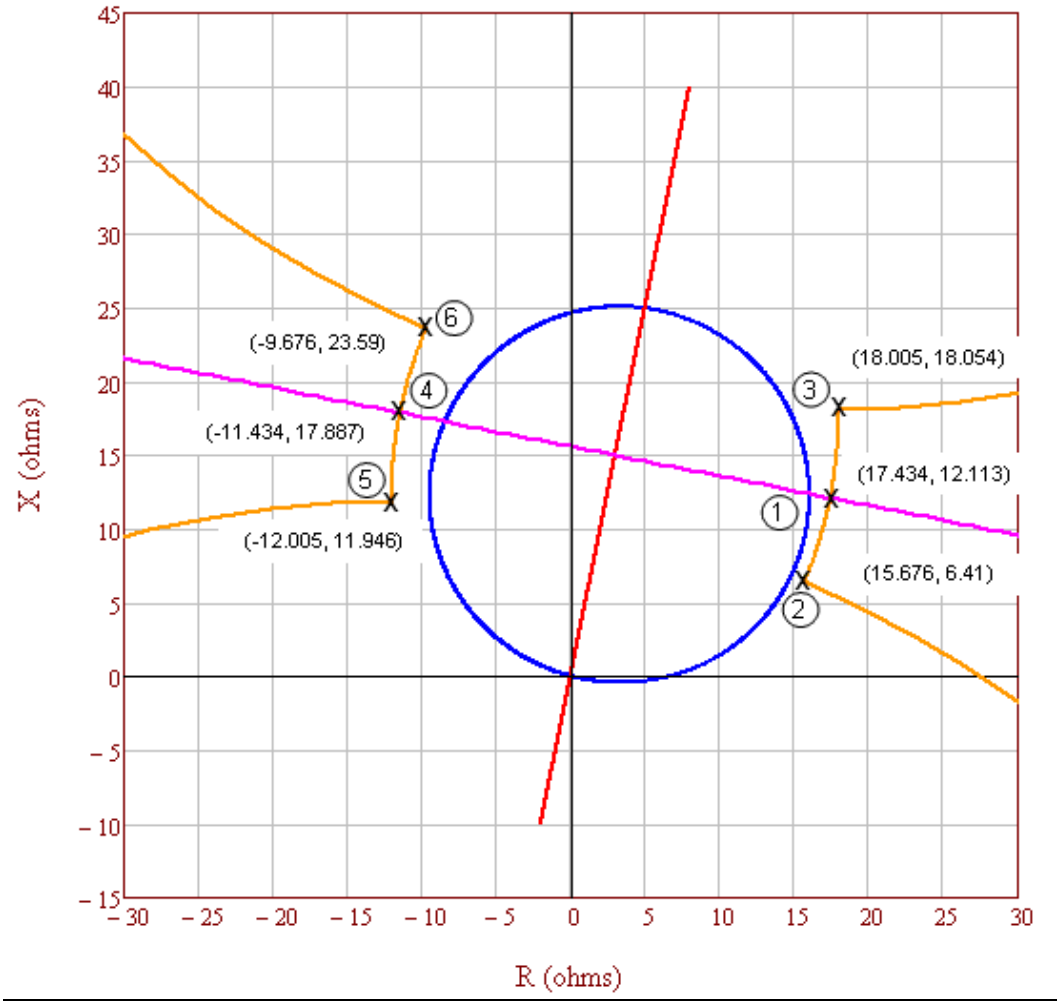


Figure 4: The defining unstable power swing region points where the lens shape intersects the lower and upper loss-of-synchronism circle shapes and where the lens intersects the equal EMF (electromotive force) power swing.

E_S / E_R Voltage Ratio	Left Side Coordinates R	Left Side Coordinates + jX	Right Side Coordinates R	Right Side Coordinates + jX
0.7	**-12.005**	**11.946**	**15.676**	**6.41**
0.72	-12.004	12.407	15.852	6.836
0.74	-11.996	12.857	16.018	7.255
0.76	-11.982	13.298	16.175	7.667
0.78	-11.961	13.729	16.321	8.073
0.8	-11.935	14.151	16.459	8.472
0.82	-11.903	14.563	16.589	8.865
0.84	-11.867	14.966	16.71	9.251
0.86	-11.826	15.361	16.824	9.631
0.88	-11.78	15.746	16.93	10.004
0.9	-11.731	16.123	17.03	10.371
0.92	-11.678	16.492	17.123	10.732
0.94	-11.621	16.852	17.209	11.086
0.96	-11.562	17.205	17.29	11.435
0.98	-11.499	17.55	17.364	11.777
1	**-11.434**	**17.887**	**17.434**	**12.113**
1.0286	-11.336	18.356	17.524	12.584
1.0572	-11.234	18.81	17.604	13.043
1.0858	-11.127	19.251	17.675	13.49
1.1144	-11.017	19.677	17.738	13.926
1.143	-10.904	20.091	17.792	14.351
1.1716	-10.788	20.491	17.84	14.766
1.2002	-10.67	20.88	17.88	15.17
1.2288	-10.55	21.256	17.914	15.564
1.2574	-10.428	21.621	17.942	15.948
1.286	-10.304	21.975	17.964	16.322
1.3146	-10.18	22.319	17.981	16.687
1.3432	-10.054	22.652	17.993	17.043
1.3718	-9.928	22.976	18.001	17.39
1.4004	-9.801	23.29	18.005	17.728
1.429	**-9.676**	**23.59**	**18.005**	**18.054**

Figure 5: Full table of 31 detailed lens shape point calculations. The bold highlighted rows correspond to the detailed calculations in Tables 2-7.

Table 2: Example Calculation (Lens Point 1)	
This example is for calculating the impedance the first point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 120 degrees. See Figures 3 and 4.	
Eq. (6)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$

Table 2: Example Calculation (Lens Point 1)			
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (7)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (8)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (9)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (10)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (11)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		

Table 2: Example Calculation (Lens Point 1)	
	$I_L = 4{,}511\angle 71.3° \; A \times \frac{(4 + j20) \times 10^{10} \; \Omega}{(4 + j20) \; \Omega + (4 + j20) \times 10^{10} \; \Omega}$
	$I_L = 4{,}511\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (12)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10) \; \Omega \times 4{,}511\angle 71.3° \; A]$
	$V_S = 95{,}757\angle 106.1° \; V$
The impedance seen by the relay on Z_L.	
Eq. (13)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \; V}{4{,}511\angle 71.3° \; A}$
	$Z_{L-Relay} = 17.434 + j12.113 \; \Omega$

Table 3: Example Calculation (Lens Point 2)			
This example is for calculating the impedance second point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (14)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 120° \; V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 120° \; V$		
Eq. (15)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \; V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \; V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10 \; \Omega$	$Z_L = 4 + j20 \; \Omega$	$Z_R = 4 + j20 \; \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10} \; \Omega$		

Table 3: Example Calculation (Lens Point 2)	
Total impedance between the generators.	
Eq. (16)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (17)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (18)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 120°\ V - 132{,}791\angle 0°\ V}{(10 + j50)\ \Omega}$
	$I_{sys} = 3{,}854\angle 77°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (19)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 77°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 77°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (20)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 92{,}953\angle 120°\ V - [(2 + j10\ )\Omega \times 3{,}854\angle 77°\ A]$
	$V_S = 65{,}271\angle 99°\ V$
The impedance seen by the relay on Z_L.	
Eq. (21)	$Z_{L-Relay} = \frac{V_S}{I_L}$

Table 3: Example Calculation (Lens Point 2)	
	$Z_{L-Relay} = \frac{65{,}271\angle 99°\ V}{3{,}854\angle 77°\ A}$
	$Z_{L-Relay} = 15.676 + j6.41\ \Omega$

Table 4: Example Calculation (Lens Point 3)			
This example is for calculating the impedance third point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 120 degrees. See Figures 3 and 4.			
Eq. (22)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (23)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (24)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (25)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		

Table 4: Example Calculation (Lens Point 3)	
Total system current from sending-end source.	
Eq. (26)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{132{,}791\angle 120° \, V - 92{,}953.7\angle 0° \, V}{(10 + j50) \, \Omega}$
	$I_{sys} = 3{,}854\angle 65.5° \, A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (27)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 65.5° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 65.5° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (28)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10) \, \Omega \times 3{,}854\angle 65.5° \, A]$
	$V_S = 98{,}265\angle 110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (29)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle 110.6° \, V}{3{,}854\angle 65.5° \, A}$
	$Z_{L-Relay} = 18.005 + j18.054 \, \Omega$

Table 5: Example Calculation (Lens Point 4)	
This example is for calculating the impedance fourth point of the lens characteristic. Equal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) leading the receiving-end voltage (E_R) by 240 degrees. See Figures 3 and 4.	
Eq. (30)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}}$

Table 5: Example Calculation (Lens Point 4)			
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (31)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (32)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (33)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (34)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 132{,}791\angle 0°\ V}{(10 + j50\ )\Omega}$		
	$I_{sys} = 4{,}511\angle 131.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (35)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 131.1°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 131.1°\ A$		

Table 5: Example Calculation (Lens Point 4)			
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.			
Eq. (36)	$V_S = E_S - (Z_S \times I_L)$		
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10\,)\,\Omega \times 4{,}511\angle 131.1° \, A]$		
	$V_S = 95{,}756\angle -106.1° \, V$		
The impedance seen by the relay on Z_L.			
Eq. (37)	$Z_{L-Relay} = \frac{V_S}{I_L}$		
	$Z_{L-Relay} = \frac{95{,}756\angle -106.1° \, V}{4{,}511\angle 131.1° \, A}$		
	$Z_{L-Relay} = -11.434 + j17.887\ \Omega$		

Table 6: Example Calculation (Lens Point 5)			
This example is for calculating the impedance fifth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the sending-end voltage (E_S) at 70% of the receiving-end voltage (E_R) and leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (38)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}} \times 70\%$		
	$E_S = \frac{230{,}000\angle 240° \, V}{\sqrt{3}} \times 0.70$		
	$E_S = 92{,}953.7\angle 240° \, V$		
Eq. (39)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0° \, V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0° \, V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (40)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		

Table 6: Example Calculation (Lens Point 5)	
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$
	$Z_{total} = 4 + j20\ \Omega$
Total system impedance.	
Eq. (41)	$Z_{sys} = Z_S + Z_{total} + Z_R$
	$Z_{sys} = (2 + j10\ \Omega) + (4 + j20\ \Omega) + (4 + j20\ \Omega)$
	$Z_{sys} = 10 + j50\ \Omega$
Total system current from sending-end source.	
Eq. (42)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$
	$I_{sys} = \frac{92{,}953.7\angle 240°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$
	$I_{sys} = 3{,}854\angle 125.5°\ A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (43)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 125.5°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$
	$I_L = 3{,}854\angle 125.5°\ A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (44)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 92{,}953.7\angle 240°\ V - [(2 + j10\ )\ \Omega \times 3{,}854\angle 125.5°\ A]$
	$V_S = 65{,}270.5\angle -99.4°\ V$
The impedance seen by the relay on Z_L.	
Eq. (45)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{65{,}270.5\angle -99.4°\ V}{3{,}854\angle 125.5°\ A}$
	$Z_{L-Relay} = -12.005 + j11.946\ \Omega$

Table 7: Example Calculation (Lens Point 6)			
This example is for calculating the impedance sixth point of the lens characteristic. Unequal source voltages are used for the 230 kV (base) line with the receiving-end voltage (E_R) at 70% of the sending-end voltage (E_S) and the sending-end voltage leading the receiving-end voltage by 240 degrees. See Figures 3 and 4.			
Eq. (46)	$E_S = \frac{V_{LL}\angle 240°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 240°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 240°\ V$		
Eq. (47)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 70\%$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 0.70$		
	$E_R = 92{,}953.7\angle 0°\ V$		
Positive sequence impedance data (with transfer impedance Z_{TR} set to a large value).			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (48)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (49)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (50)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 240°\ V - 92{,}953.7\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 3{,}854\angle 137.1°\ A$		

Table 7: Example Calculation (Lens Point 6)	
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (51)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 3{,}854\angle 137.1° \, A \times \frac{(4 + j20) \times 10^{10} \, \Omega}{(4 + j20) \, \Omega + (4 + j20) \times 10^{10} \, \Omega}$
	$I_L = 3{,}854\angle 137.1° \, A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (52)	$V_S = E_S - (Z_S \times I_L)$
	$V_S = 132{,}791\angle 240° \, V - [(2 + j10 \,) \, \Omega \times 3{,}854\angle 137.1° \, A]$
	$V_S = 98{,}265\angle -110.6° \, V$
The impedance seen by the relay on Z_L.	
Eq. (53)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{98{,}265\angle -110.6° \, V}{3{,}854\angle 137.1° \, A}$
	$Z_{L-Relay} = -9.676 + j23.59 \, \Omega$

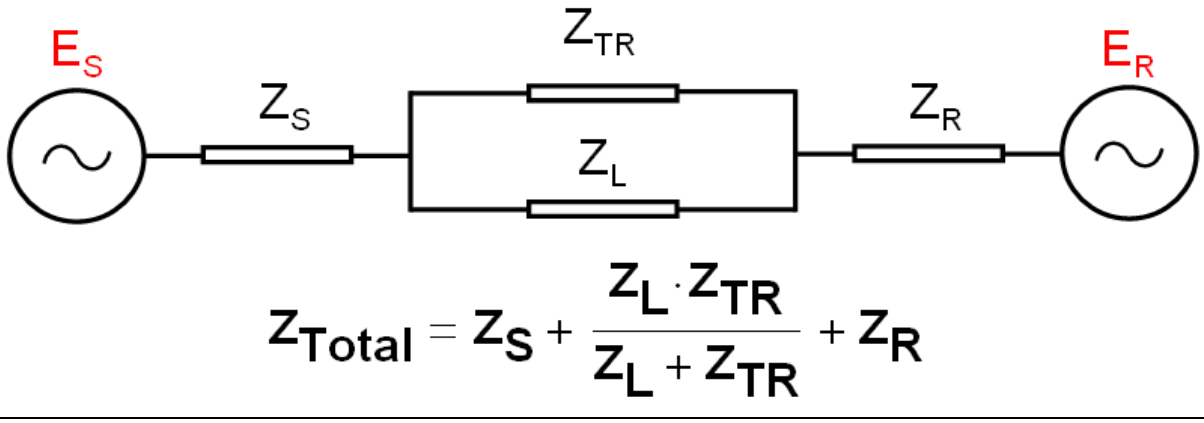


Figure 6: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, line impedance Z_L, and parallel transfer impedance Z_{TR}.

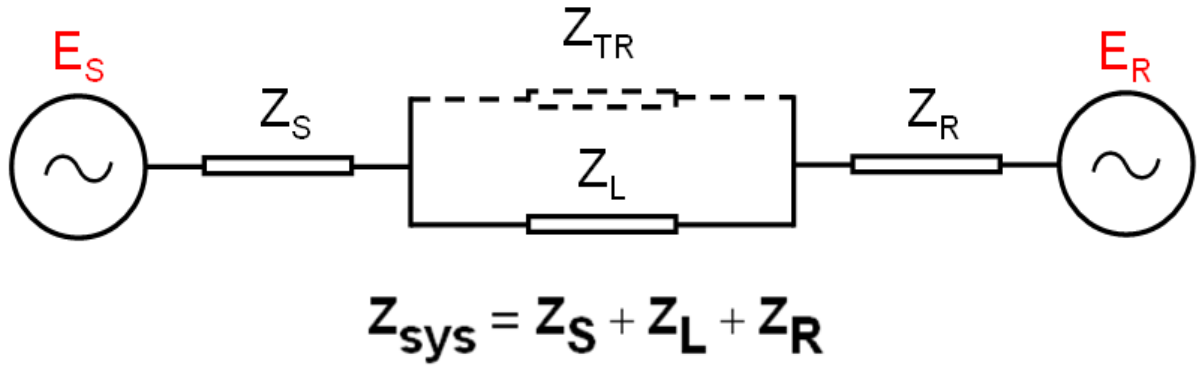


Figure 7: Reduced two bus system with sending-end source impedance Z_S, receiving-end source impedance Z_R, and line impedance Z_L with the parallel transfer impedance Z_{TR} removed.

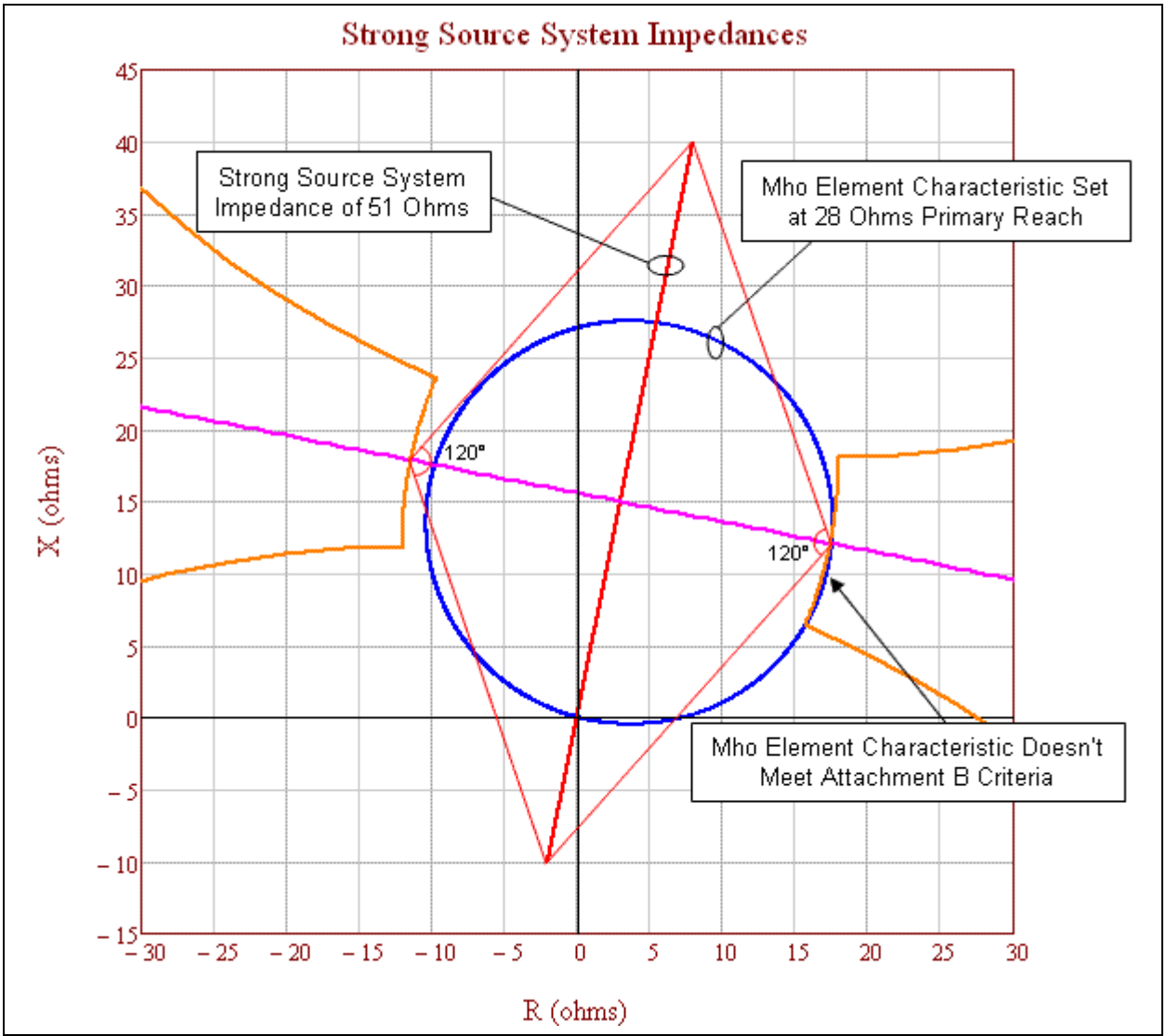


Figure 8: A strong-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) does not meet the PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 8 above represents a heavily-loaded system with all generation in service and all transmission BES Elements in their normal operating state. The mho element characteristic (set at 137% of Z_L) extends into the unstable power swing region (i.e., the orange characteristic). Using the strongest source system is more conservative because it shrinks the unstable power swing region, bringing it closer to the mho element characteristic. This figure also graphically represents the effect of a system strengthening over time and this is the reason for re-evaluation if the relay has not been evaluated in the last five calendar years. Figure 9 below depicts a relay that meets the PRC-026-1 – Attachment B, Criterion A. Figure 8 depicts the same relay with the same setting five years later, where each source has strengthened by about 10% and now the same mho element characteristic does not meet Criterion A.

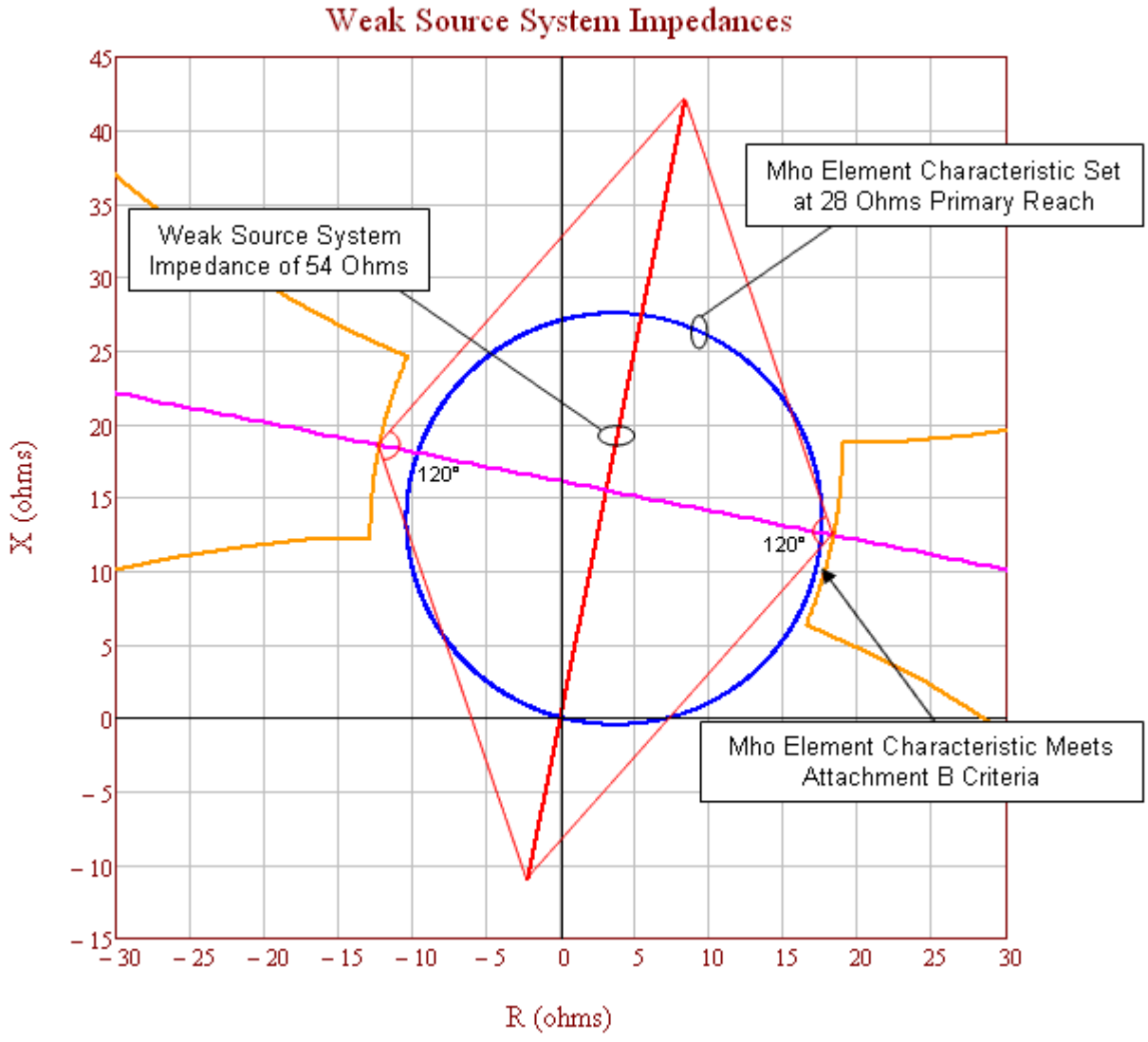


Figure 9: A weak-source system with a line impedance of Z_L = 20.4 ohms (i.e., the thicker red line). This mho element characteristic (i.e., the blue circle) meets the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region (i.e., the orange characteristic).

Figure 9 above represents a lightly-loaded system, using a minimum generation profile. The mho element characteristic (set at 137% of Z_L) does not extend into the unstable power swing region (i.e., the orange characteristic). Using a weaker source system expands the unstable power swing region away from the mho element characteristic.

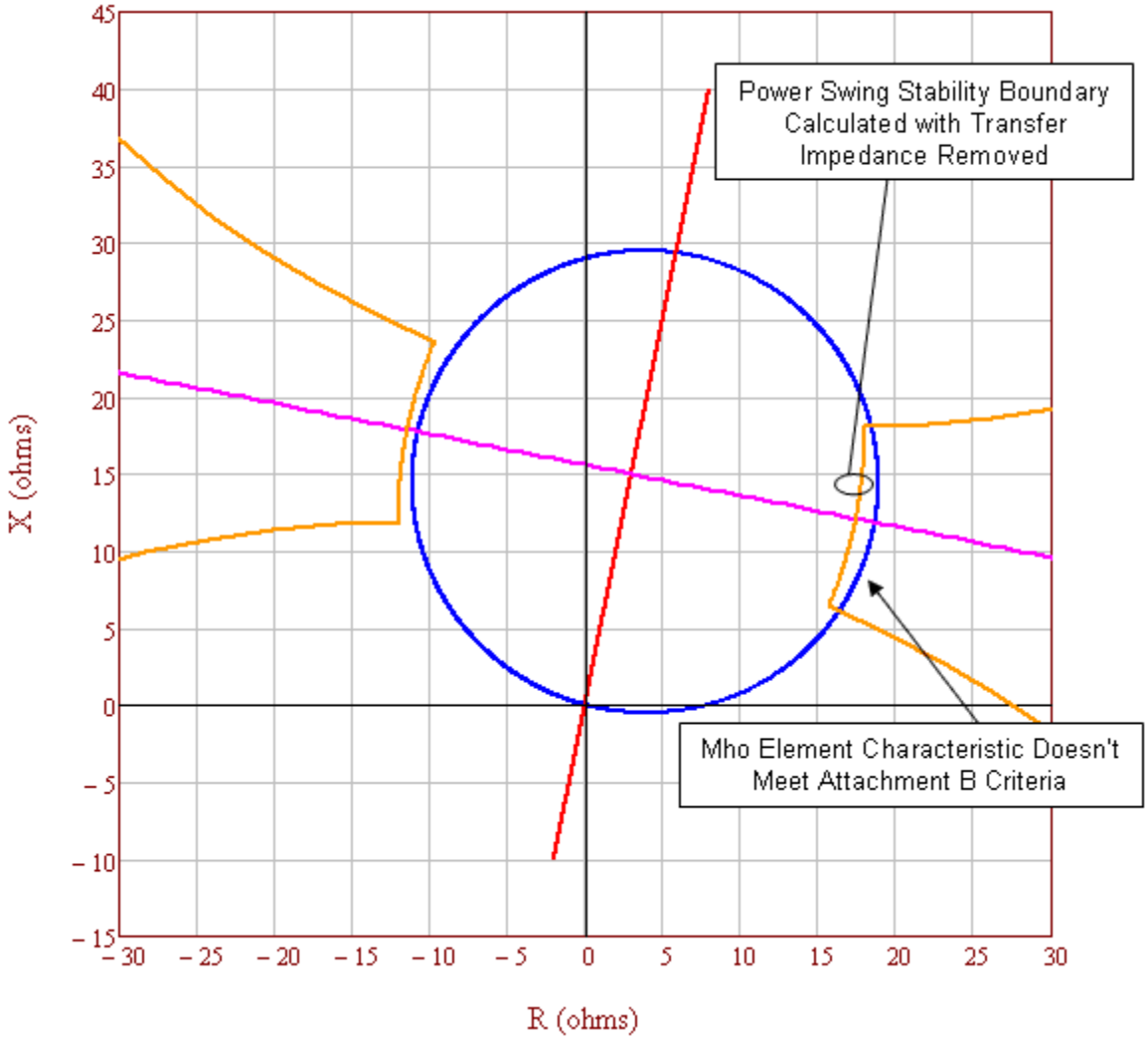


Figure 10: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance removed. This relay mho element characteristic (i.e., the blue circle) does not meet PRC-026-1 – Attachment B, Criterion A because it is not completely contained within the unstable power swing region.

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
Calculations for the point at 120 degrees with equal source impedances. The total system current equals the line current. See Figure 10.	
Eq. (54)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$
	$E_S = 132{,}791\angle 120°\ V$

Table 8: Example Calculation (Parallel Transfer Impedance Removed)			
Eq. (55)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
Total impedance between the generators.			
Eq. (56)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{\left((4 + j20)\ \Omega \times (4 + j20) \times 10^{10}\ \Omega\right)}{\left((4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega\right)}$		
	$Z_{total} = 4 + j20\ \Omega$		
Total system impedance.			
Eq. (57)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (4 + j20)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 10 + j50\ \Omega$		
Total system current from sending-end source.			
Eq. (58)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{10 + j50\ \Omega}$		
	$I_{sys} = 4{,}511\angle 71.3°\ A$		
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.			
Eq. (59)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$		
	$I_L = 4{,}511\angle 71.3°\ A \times \frac{(4 + j20) \times 10^{10}\ \Omega}{(4 + j20)\ \Omega + (4 + j20) \times 10^{10}\ \Omega}$		
	$I_L = 4{,}511\angle 71.3°\ A$		

Table 8: Example Calculation (Parallel Transfer Impedance Removed)	
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (60)	$V_S = E_S - \left(Z_S \times I_{sys}\right)$
	$V_S = 132{,}791\angle 120° \, V - [(2 + j10\ \Omega) \times 4{,}511\angle 71.3° \, A]$
	$V_S = 95{,}757\angle 106.1° \, V$
The impedance seen by the relay on Z_L.	
Eq. (61)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{95{,}757\angle 106.1° \, V}{4{,}511\angle 71.3° \, A}$
	$Z_{L-Relay} = 17.434 + j12.113\ \Omega$

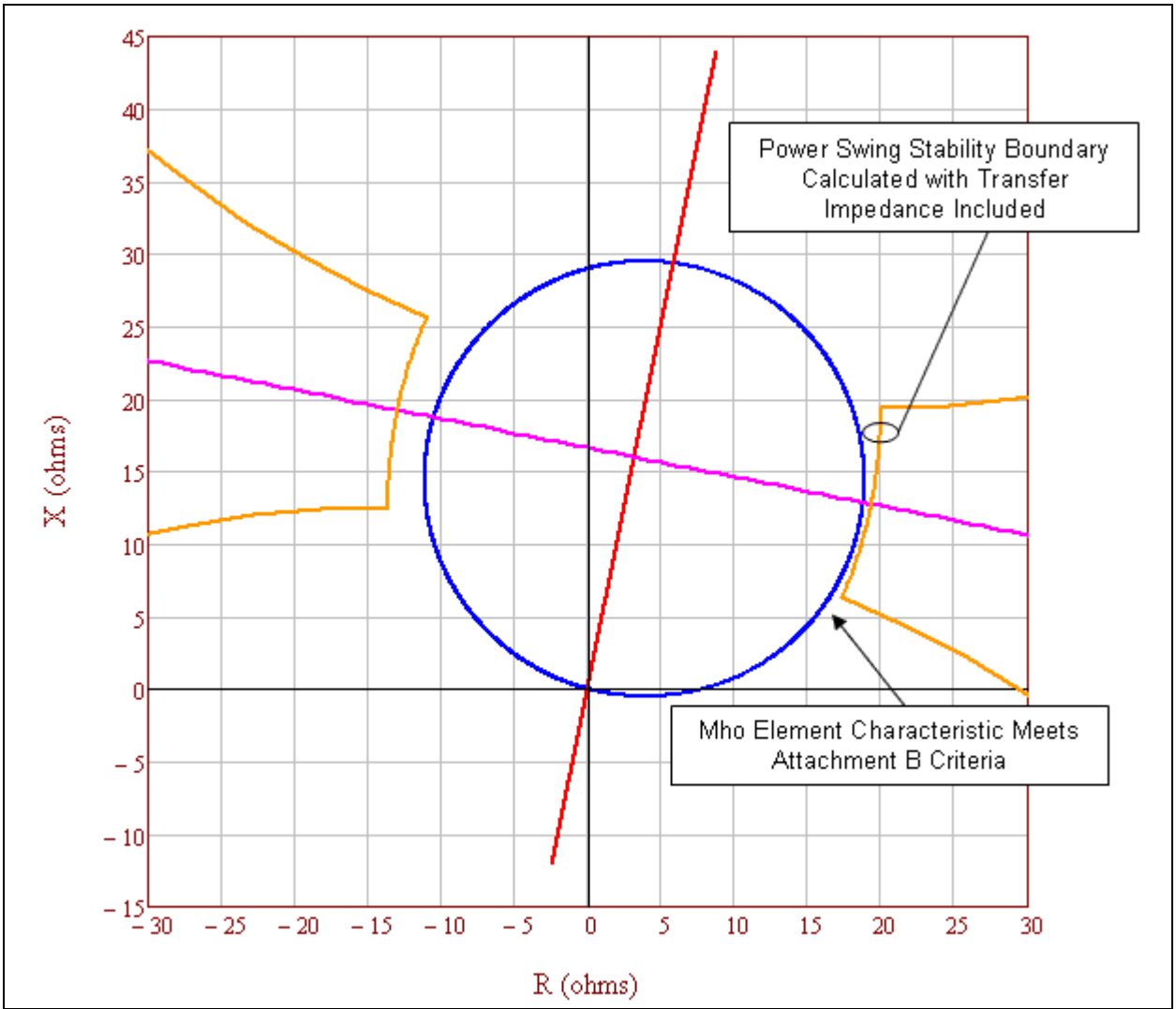


Figure 11: This is an example of an unstable power swing region (i.e., the orange characteristic) with the parallel transfer impedance included causing the mho element characteristic (i.e., the blue circle) to appear to meet the PRC-026-1 – Attachment B, Criterion A because it is completely contained within the unstable power swing region. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

In Figure 11 above, the parallel transfer impedance is 5 times the line impedance. The unstable power swing region has expanded out beyond the mho element characteristic due to the infeed effect from the parallel current through the parallel transfer impedance, thus allowing the mho element characteristic to appear to meet the PRC-026-1 – Attachment B, Criterion A. Including the parallel transfer impedance in the calculation is not allowed by the PRC-026-1 – Attachment B, Criterion A.

Table 9: Example Calculation (Parallel Transfer Impedance Included)			
Calculations for the point at 120 degrees with equal source impedances. The total system current does not equal the line current. See Figure 11.			
Eq. (62)	$E_S = \frac{V_{LL}\angle 120°}{\sqrt{3}}$		
	$E_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}}$		
	$E_S = 132{,}791\angle 120°\ V$		
Eq. (63)	$E_R = \frac{V_{LL}\angle 0°}{\sqrt{3}}$		
	$E_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}}$		
	$E_R = 132{,}791\angle 0°\ V$		
Given impedance data.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 5$		
	$Z_{TR} = (4 + j20)\ \Omega \times 5$		
	$Z_{TR} = 20 + j100\ \Omega$		
Total impedance between the generators.			
Eq. (64)	$Z_{total} = \frac{(Z_L \times Z_{TR})}{(Z_L + Z_{TR})}$		
	$Z_{total} = \frac{(4 + j20)\ \Omega \times (20 + j100)\ \Omega}{(4 + j20)\ \Omega + (20 + j100)\ \Omega}$		
	$Z_{total} = 3.333 + j16.667\ \Omega$		
Total system impedance.			
Eq. (65)	$Z_{sys} = Z_S + Z_{total} + Z_R$		
	$Z_{sys} = (2 + j10)\ \Omega + (3.333 + j16.667)\ \Omega + (4 + j20)\ \Omega$		
	$Z_{sys} = 9.333 + j46.667\ \Omega$		
Total system current from sending-end source.			
Eq. (66)	$I_{sys} = \frac{E_S - E_R}{Z_{sys}}$		
	$I_{sys} = \frac{132{,}791\angle 120°\ V - 132{,}791\angle 0°\ V}{9.333 + j46.667\ \Omega}$		

Table 9: Example Calculation (Parallel Transfer Impedance Included)	
	$I_{sys} = 4{,}833\angle 71.3° \; A$
The current, as measured by the relay on Z_L (Figure 3), is only the current flowing through that line as determined by using the current divider equation.	
Eq. (67)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$
	$I_L = 4{,}833\angle 71.3° \; A \times \frac{(20 + j100)\ \Omega}{(4 + j20)\ \Omega + (20 + j100)\ \Omega}$
	$I_L = 4{,}027.4\angle 71.3° \; A$
The voltage, as measured by the relay on Z_L (Figure 3), is the voltage drop from the sending-end source through the sending-end source impedance.	
Eq. (68)	$V_S = E_S - (Z_S \times I_{sys})$
	$V_S = 132{,}791\angle 120° \; V - [(2 + j10\ \Omega) \times 4{,}833\angle 71.3° \; A]$
	$V_S = 93{,}417\angle 104.7° \; V$
The impedance seen by the relay on Z_L.	
Eq. (69)	$Z_{L-Relay} = \frac{V_S}{I_L}$
	$Z_{L-Relay} = \frac{93{,}417\angle 104.7° \; V}{4{,}027\angle 71.3° \; A}$
	$Z_{L-Relay} = 19.366 + j12.767\ \Omega$

Table 10: Percent Increase of a Lens Due To Parallel Transfer Impedance.	
The following demonstrates the percent size increase of the lens characteristic for Z_{TR} in multiples of Z_L with the parallel transfer impedance included.	
Z_{TR} in multiples of Z_L	Percent increase of lens with equal EMF sources (Infinite source as reference)
Infinite	N/A
1000	0.05%
100	0.46%
10	4.63%
5	9.27%
2	23.26%
1	46.76%
0.5	94.14%
0.25	189.56%

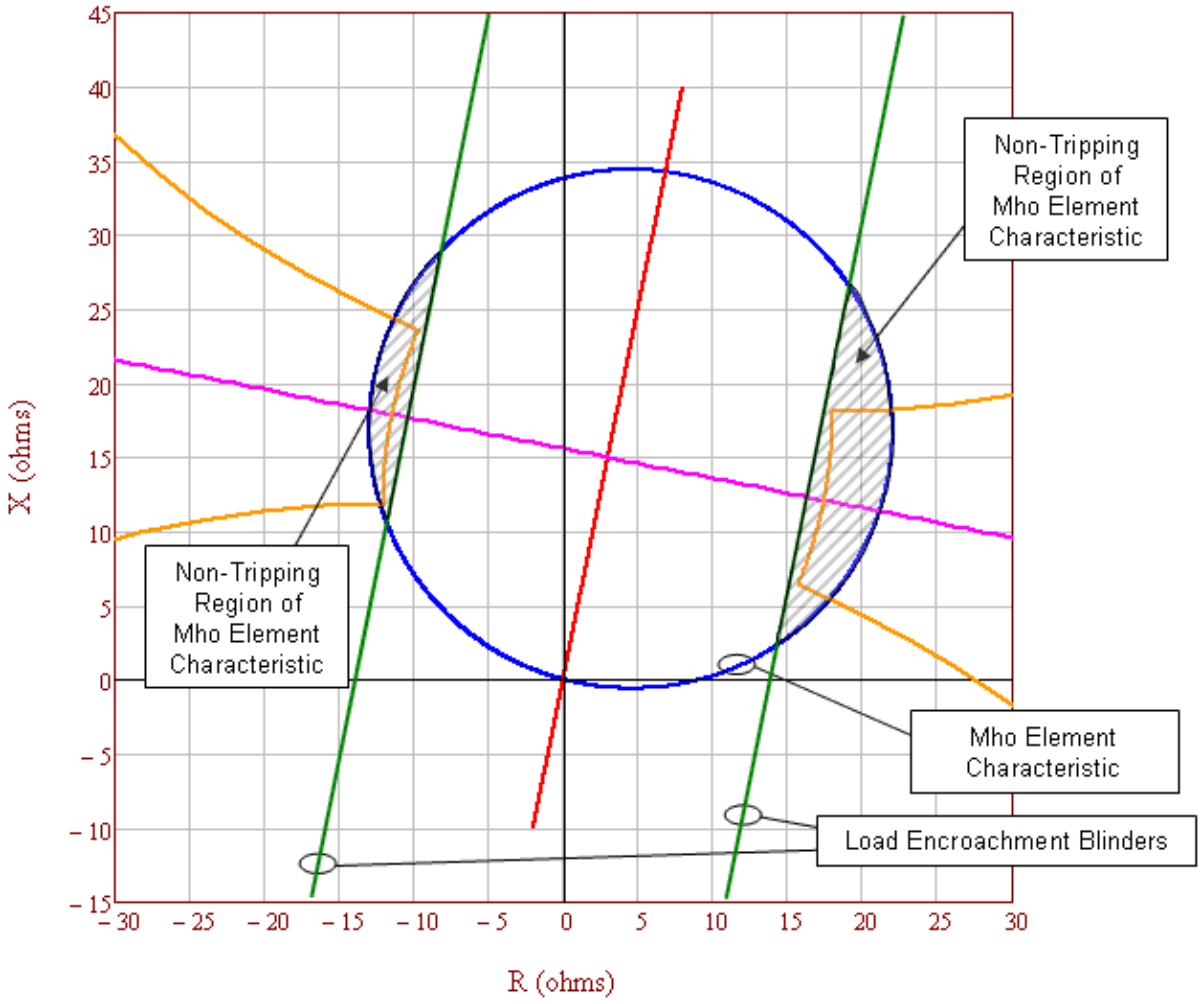


Figure 12: The tripping portion of the mho element characteristic (i.e., the blue circle) not blocked by load encroachment (i.e., the parallel green lines) is completely contained within the unstable power swing region (i.e., the orange characteristic). Therefore, the mho element characteristic meets the PRC-026-1 – Attachment B, Criterion A.

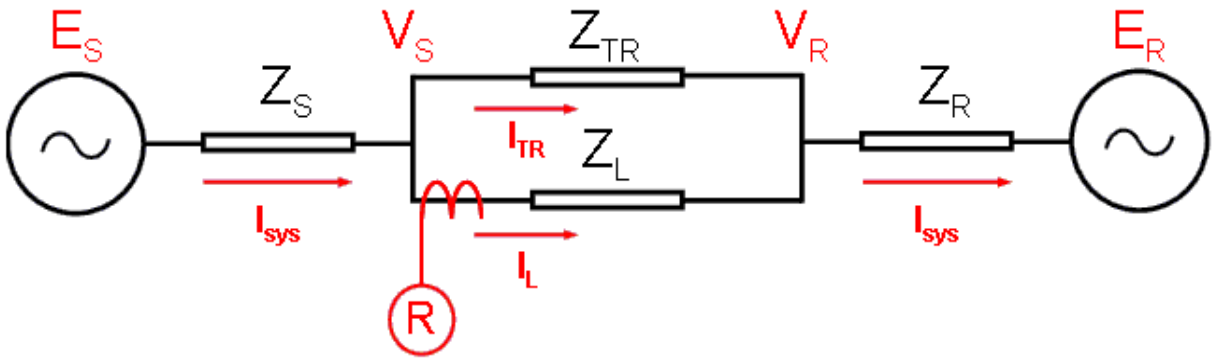


Figure 13: The infeed diagram shows the impedance in front of the relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.

Table 11: Calculations (System Apparent Impedance in the forward direction)

The following equations are provided for calculating the apparent impedance back to the E_R source voltage as seen by relay R. Infeed equations from V_S to source E_R where $E_R = 0$. See Figure 13.

Eq. (70)	$I_L = \frac{V_S - V_R}{Z_L}$			
Eq. (71)	$I_{sys} = \frac{V_R - E_R}{Z_R}$			
Eq. (72)	$I_{sys} = I_L + I_{TR}$			
Eq. (73)	$I_{sys} = \frac{V_R}{Z_R}$	Since $E_R = 0$	Rearranged:	$V_R = I_{sys} \times Z_R$
Eq. (74)	$I_L = \frac{V_S - I_{sys} \times Z_R}{Z_L}$			
Eq. (75)	$I_L = \frac{V_S - [(I_L + I_{TR}) \times Z_R]}{Z_L}$			
Eq. (76)	$V_S = (I_L \times Z_L) + (I_L \times Z_R) + (I_{TR} \times Z_R)$			
Eq. (77)	$Z_{Relay} = \frac{V_S}{I_L} = Z_L + Z_R + \frac{I_{TR} \times Z_R}{I_L} = Z_L + Z_R \times \left(1 + \frac{I_{TR}}{I_L}\right)$			
Eq. (78)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$			
Eq. (79)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$			

Table 11: Calculations (System Apparent Impedance in the forward direction)	
Eq. (80)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$
The infeed equations shows the impedance in front of the relay R (Figure 13) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the forward direction becomes $Z_L + Z_R$.	
Eq. (81)	$Z_{Relay} = Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$

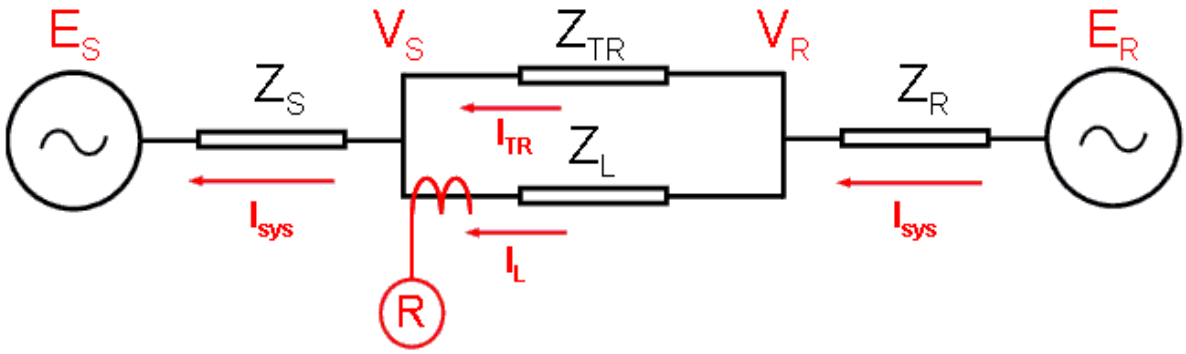


Figure 14: The infeed diagram shows the impedance behind relay R with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)				
The following equations are provided for calculating the apparent impedance back to the E_S source voltage as seen by relay R. Infeed equations from V_R back to source E_S where $E_S = 0$. See Figure 14.				
Eq. (82)	$I_L = \frac{V_R - V_S}{Z_L}$			
Eq. (83)	$I_{sys} = \frac{V_S - E_S}{Z_S}$			
Eq. (84)	$I_{sys} = I_L + I_{TR}$			
Eq. (85)	$I_{sys} = \frac{V_S}{Z_S}$	Since $E_s = 0$	Rearranged:	$V_S = I_{sys} \times Z_S$
Eq. (86)	$I_L = \frac{V_R - I_{sys} \times Z_S}{Z_L}$			

Table 12: Calculations (System Apparent Impedance in the Reverse Direction)		
Eq. (87)	$I_L = \frac{V_R - [(I_L + I_{TR}) \times Z_S]}{Z_L}$	
Eq. (88)	$V_R = (I_L \times Z_L) + (I_L \times Z_S) + (I_{TR} \times Z_{RS})$	
Eq. (89)	$Z_{Relay} = \frac{V_R}{I_L} = Z_L + Z_S + \frac{I_{TR} \times Z_S}{I_L} = Z_L + Z_S \times \left(1 + \frac{I_{TR}}{I_L}\right)$	
Eq. (90)	$I_{TR} = I_{sys} \times \frac{Z_L}{Z_L + Z_{TR}}$	
Eq. (91)	$I_L = I_{sys} \times \frac{Z_{TR}}{Z_L + Z_{TR}}$	
Eq. (92)	$\frac{I_{TR}}{I_L} = \frac{Z_L}{Z_{TR}}$	
The infeed equations shows the impedance behind relay R (Figure 14) with the parallel transfer impedance included. As the parallel transfer impedance approaches infinity, the impedances seen by the relay R in the reverse direction becomes Z_S.		
Eq. (93)	$Z_{Relay} = Z_L + Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	As seen by relay R at the receiving-end of the line.
Eq. (94)	$Z_{Relay} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)$	Subtract Z_L for relay R impedance as seen at sending-end of the line.

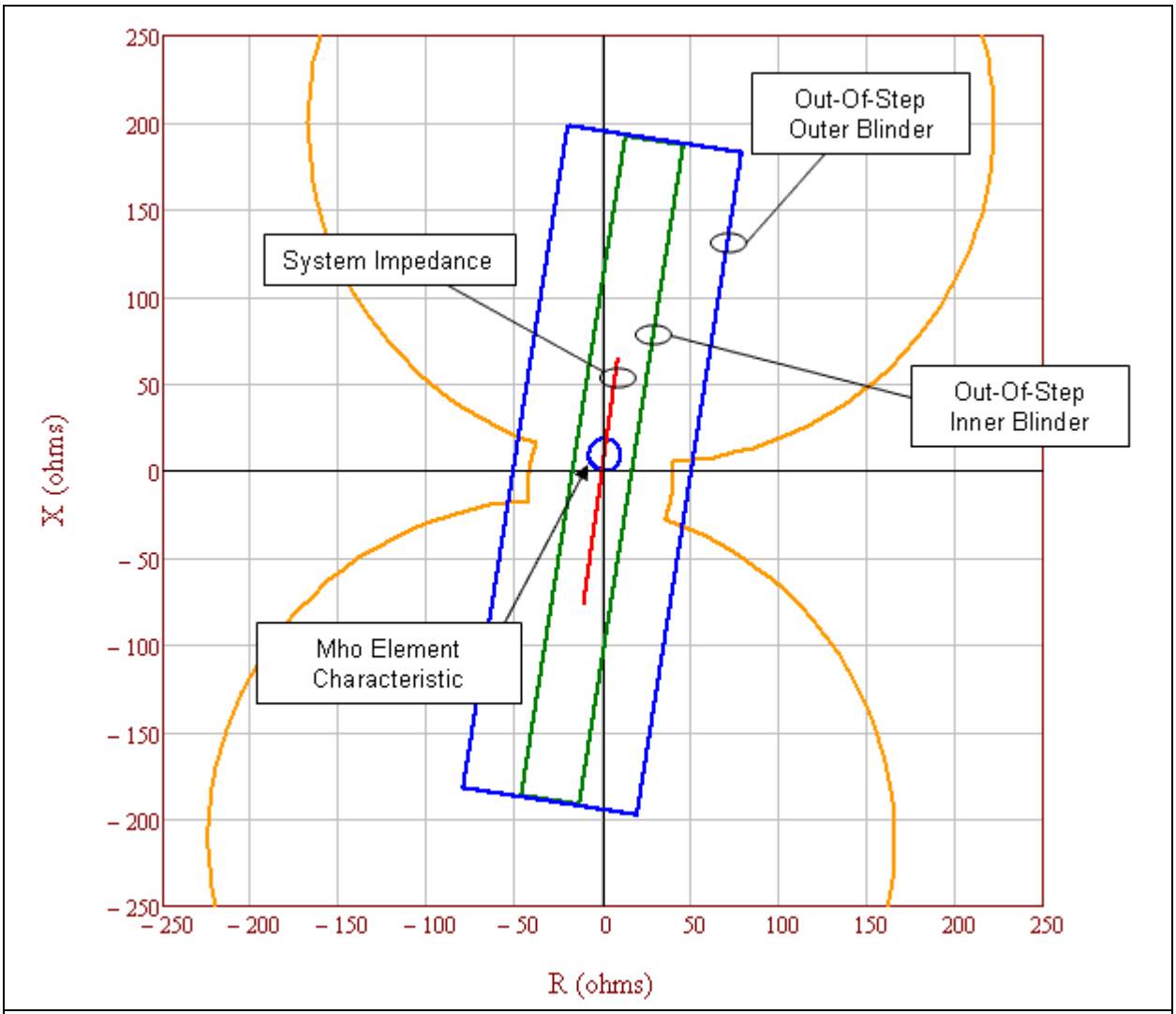


Figure 15: Out-of-step trip (OST) inner blinder (i.e., the parallel green lines) meets the PRC-026-1 – Attachment B, Criterion A because the inner OST blinder initiates tripping either On-The-Way-In or On-The-Way-Out. Since the inner blinder is completely contained within the unstable power swing region (i.e., the orange characteristic), it meets the PRC-026-1 – Attachment B, Criterion A.

Table 13: Example Calculation (Voltage Ratios)			
These calculations are based on the loss-of-synchronism characteristics for the cases of N < 1 and N > 1 as found in the *Application of Out-of-Step Blocking and Tripping Relays*, GER-3180, p. 12, Figure 3.[18] The GE illustration shows the formulae used to calculate the radius and center of the circles that make up the ends of the portion of the lens.			
Voltage ratio equations, source impedance equation with infeed formulae applied, and circle equations.			
Given:	$E_S = 0.7$	$E_R = 1.0$	
Eq. (95)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{0.7}{1.0} = 0.7$		
The total system impedance as seen by the relay with infeed formulae applied.			
Given:	$Z_S = 2 + j10\ \Omega$	$Z_L = 4 + j20\ \Omega$	$Z_R = 4 + j20\ \Omega$
Given:	$Z_{TR} = Z_L \times 10^{10}\ \Omega$		
	$Z_{TR} = (4 + j20) \times 10^{10}\ \Omega$		
Eq. (96)	$Z_{sys} = Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right) + \left[Z_L + Z_R \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right]$		
	$Z_{sys} = 10 + j50\ \Omega$		
The calculated coordinates of the lower loss-of-synchronism circle center.			
Eq. (97)	$Z_{C1} = -\left[Z_S \times \left(1 + \frac{Z_L}{Z_{TR}}\right)\right] - \left[\frac{N^2 \times Z_{sys}}{1 - N^2}\right]$		
	$Z_{C1} = -\left[(2 + j10)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega}\right)\right] - \left[\frac{0.7^2 \times (10 + j50)\ \Omega}{1 - 0.7^2}\right]$		
	$Z_{C1} = -11.608 - j58.039\ \Omega$		
The calculated radius of the lower loss-of-synchronism circle.			
Eq. (98)	$r_a = \left\lvert \frac{N \times Z_{sys}}{1 - N^2} \right\rvert$		
	$r_a = \left\lvert \frac{0.7 \times (10 + j50)\ \Omega}{1 - 0.7^2} \right\rvert$		
	$r_a = 69.987\ \Omega$		
The calculated coordinates of the upper loss-of-synchronism circle center.			
Given:	$E_S = 1.0$	$E_R = 0.7$	

[18] http://store.gedigitalenergy.com/faq/Documents/Alps/GER-3180.pdf

Table 13: Example Calculation (Voltage Ratios)	
Eq. (99)	$N = \frac{\lvert E_S \rvert}{\lvert E_R \rvert} = \frac{1.0}{0.7} = 1.43$
Eq. (100)	$Z_{C2} = Z_L + \left[Z_R \times \left(1 + \frac{Z_L}{Z_{TR}} \right) \right] + \left[\frac{Z_{sys}}{N^2 - 1} \right]$
	$Z_{C2} = 4 + j20\ \Omega + \left[(4 + j20)\ \Omega \times \left(1 + \frac{(4 + j20)\ \Omega}{(4 + j20) \times 10^{10}\ \Omega} \right) \right] + \left[\frac{(10 + j50)\ \Omega}{1.43^2 - 1} \right]$
	$Z_{C2} = 17.608 + j88.039\ \Omega$
The calculated radius of the upper loss-of-synchronism circle.	
Eq. (101)	$r_b = \left\lvert \frac{N \times Z_{sys}}{N^2 - 1} \right\rvert$
	$r_b = \left\lvert \frac{1.43 \times (10 + j50)\ \Omega}{1.43^2 - 1} \right\rvert$
	$r_b = 69.987\ \Omega$

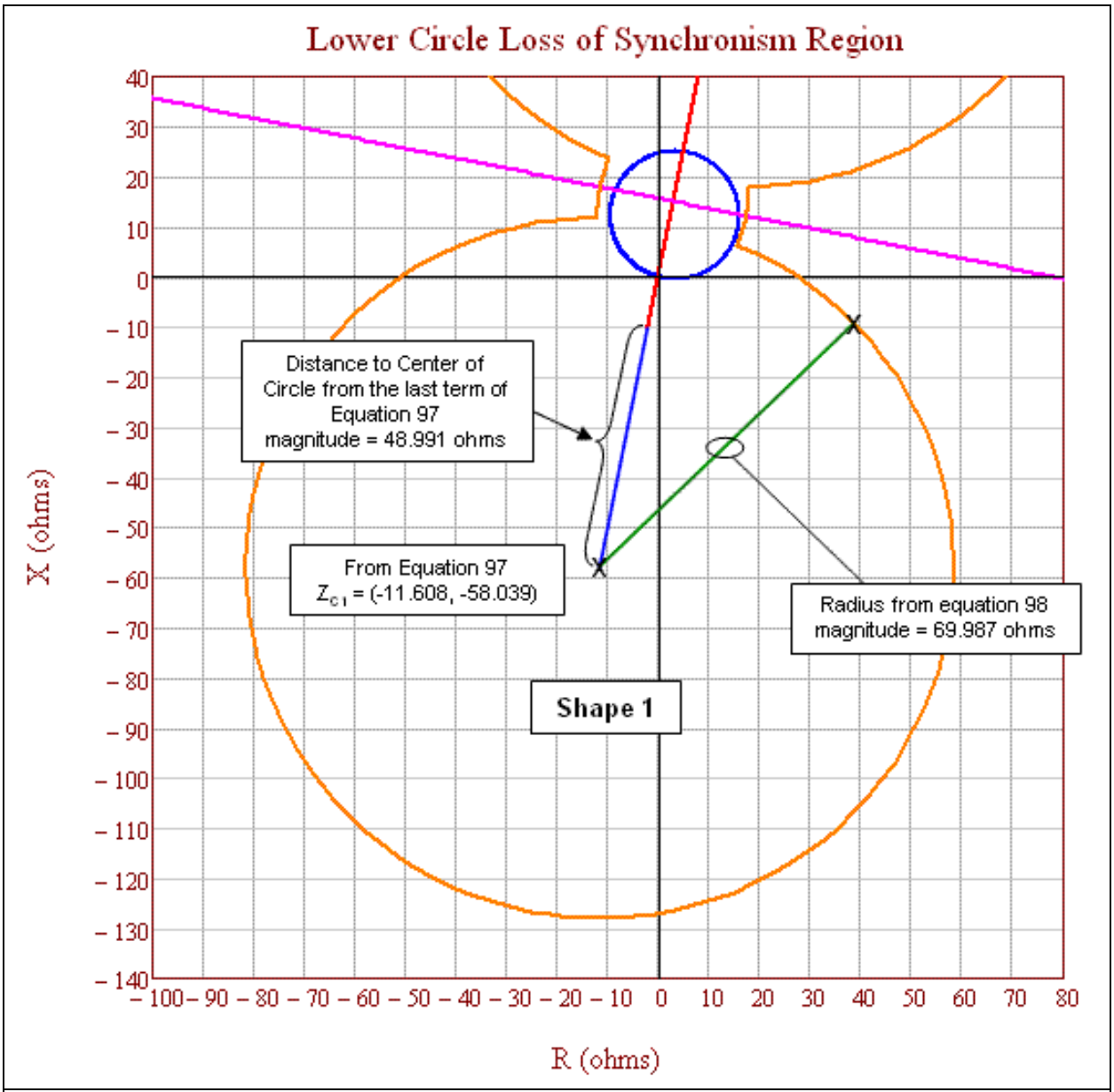


Figure 15a: Lower circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

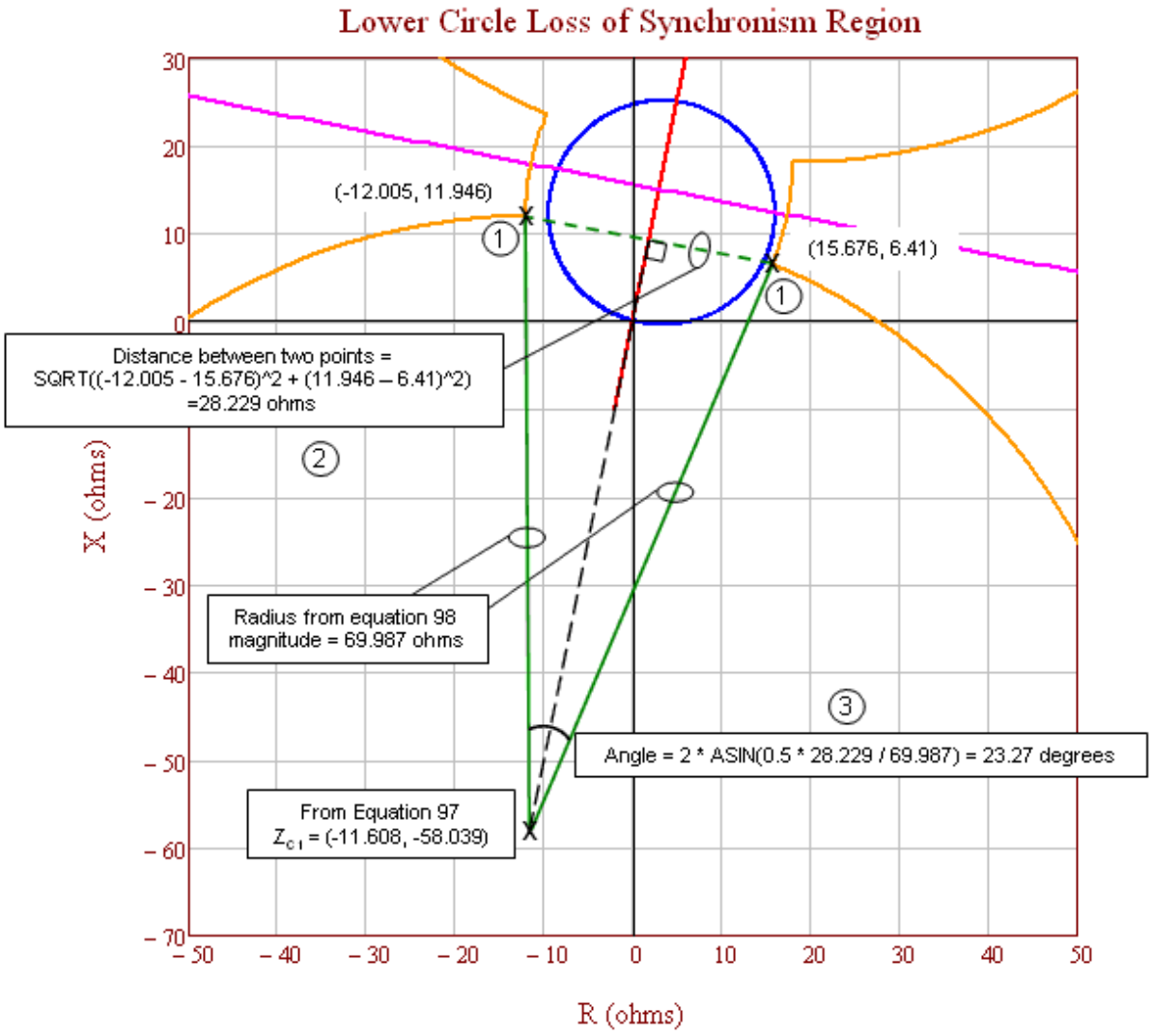


Figure 15b: Lower circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the lower circle loss-of-synchronism points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 0.7 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two lower circle loss-of-synchronism points identified in Step 1. 3) Calculate the angle of arc that connects the two lower circle loss-of-synchronism points identified in Step 1.

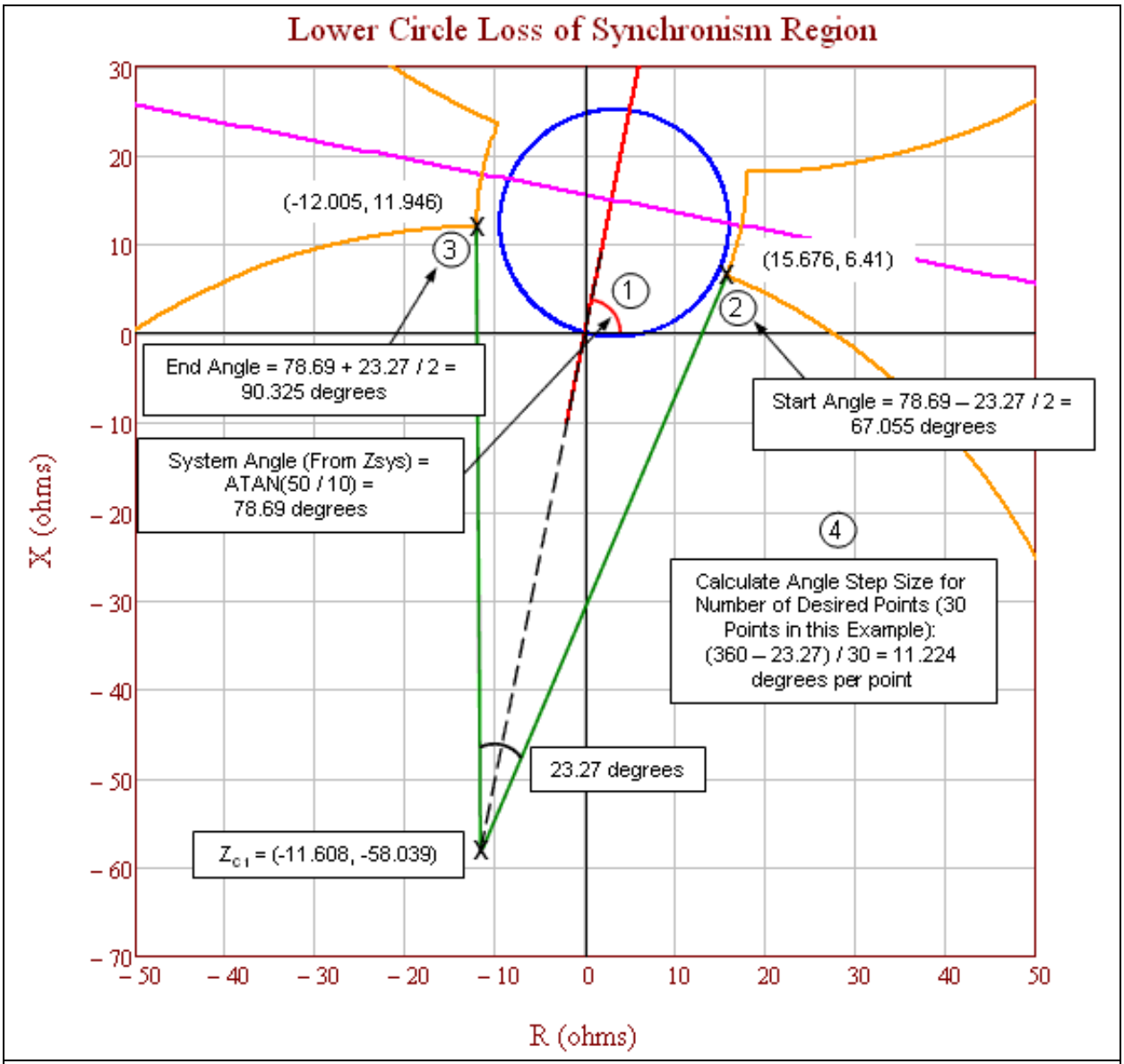


Figure 15c: Lower circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

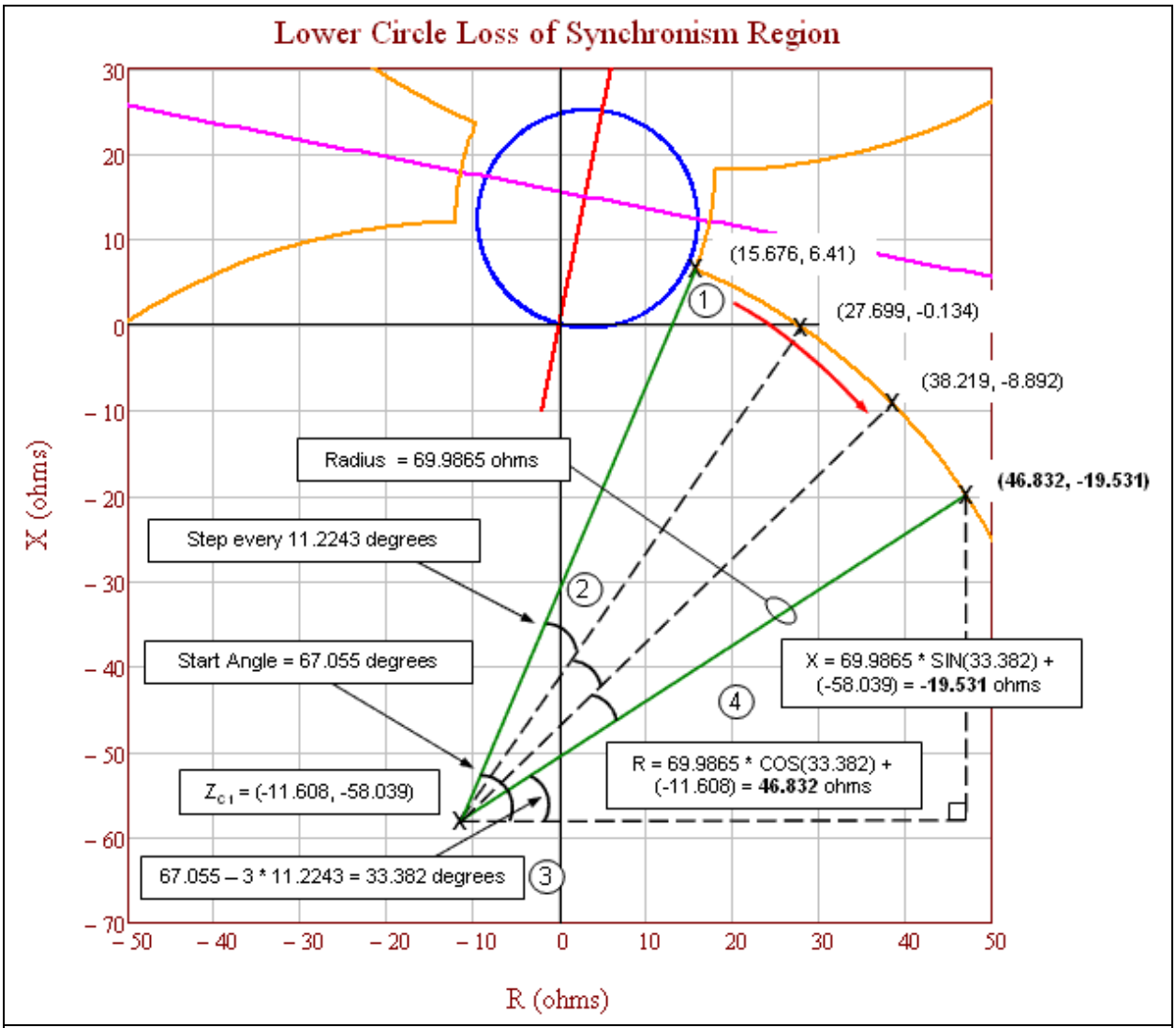


Figure 15d: Lower circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R–X coordinates.

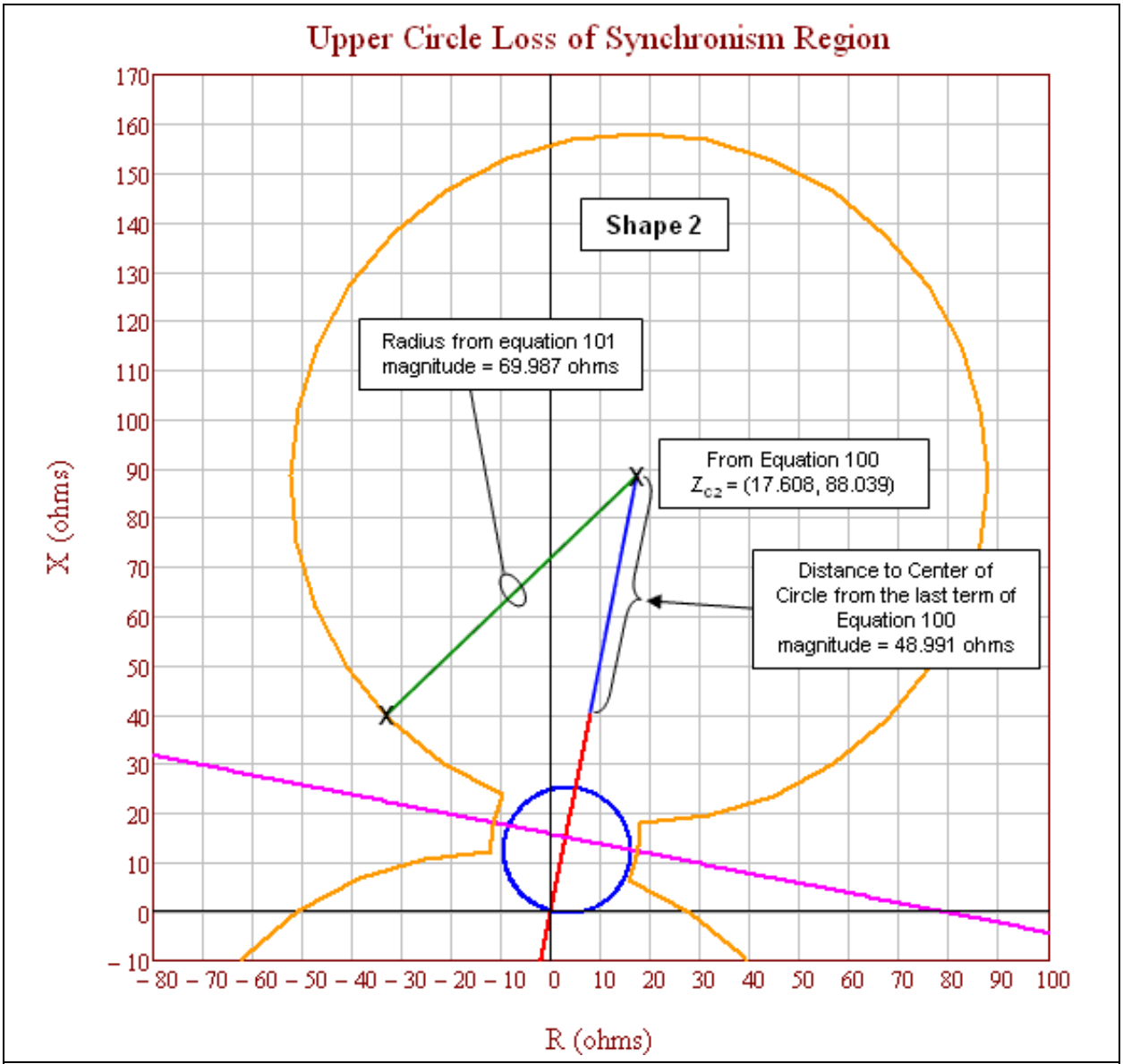


Figure 15e: Upper circle loss-of-synchronism region showing the coordinates of the circle center and the circle radius.

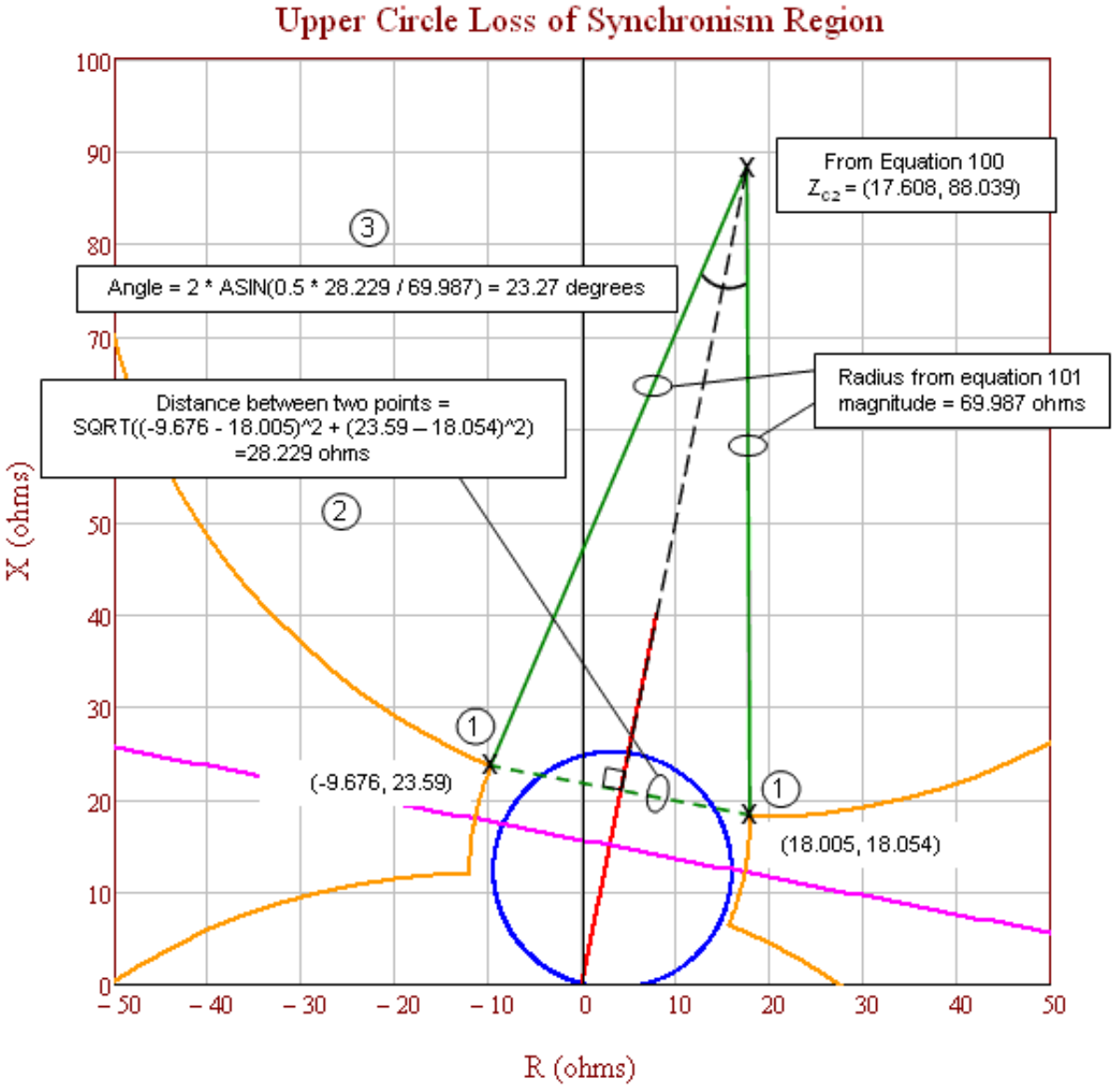


Figure 15f: Upper circle loss-of-synchronism region showing the first three steps to calculate the coordinates of the points on the circle. 1) Identify the upper circle points that intersect the lens shape where the sending-end to receiving-end voltage ratio is 1.43 (see lens shape calculations in Tables 2-7). 2) Calculate the distance between the two upper circle points identified in Step 1. 3) Calculate the angle of arc that connects the two upper circle points identified in Step 1.

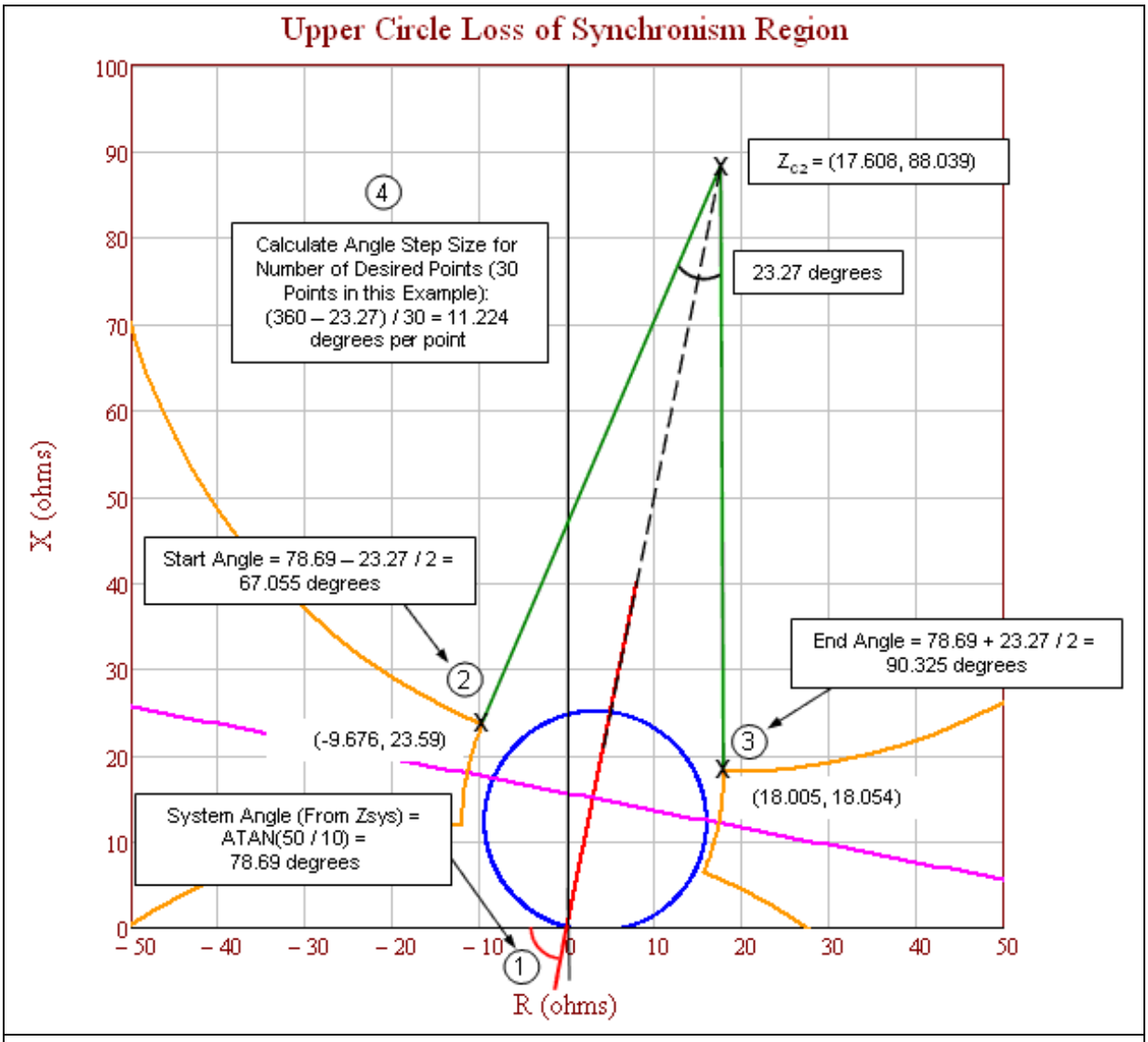


Figure 15g: Upper circle loss-of-synchronism region showing the steps to calculate the start angle, end angle, and the angle step size for the desired number of calculated points. 1) Calculate the system angle. 2) Calculate the start angle. 3) Calculate the end angle. 4) Calculate the angle step size for the desired number of points.

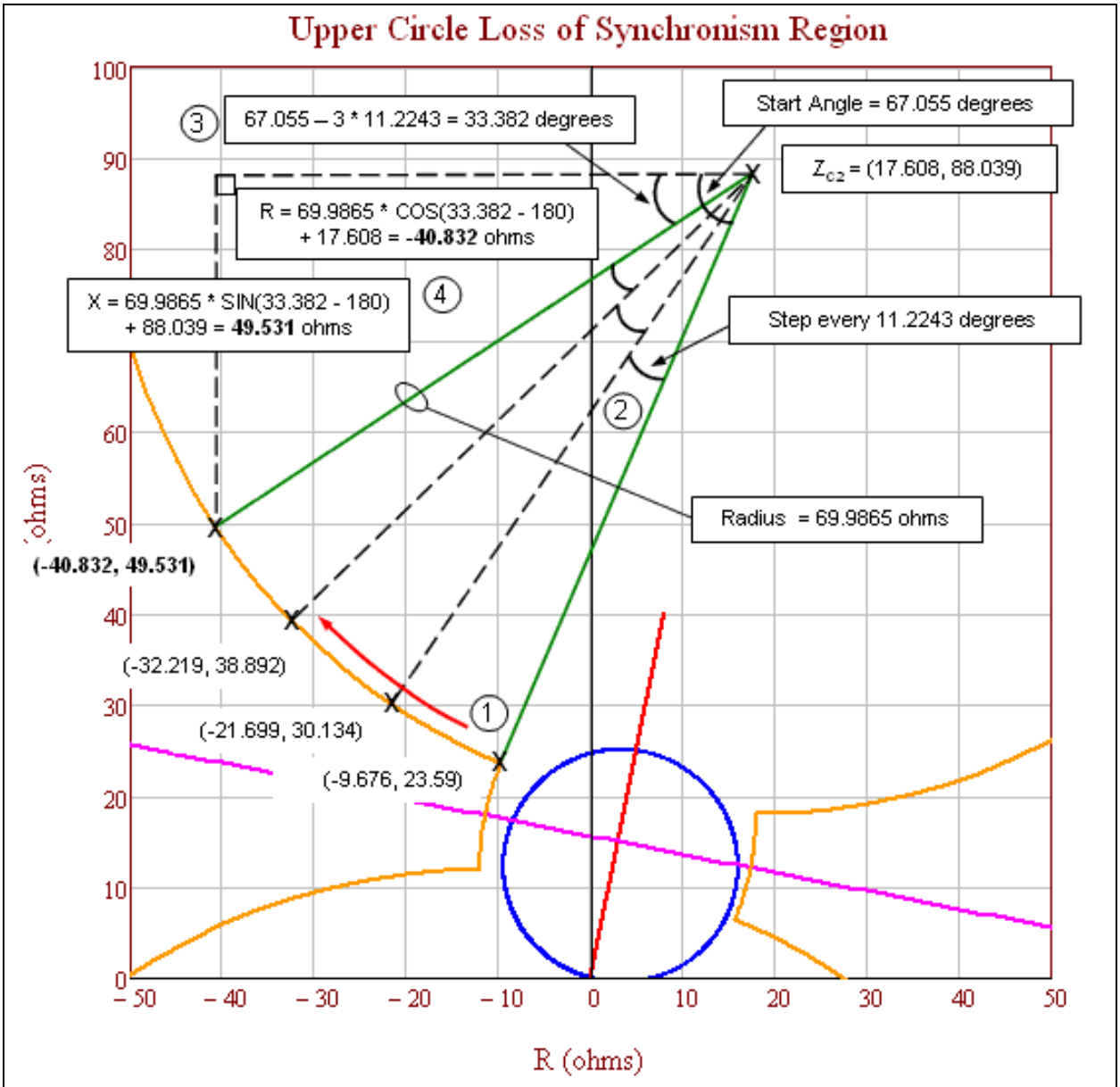


Figure 15h: Upper circle loss-of-synchronism region showing the final steps to calculate the coordinates of the points on the circle. 1) Start at the intersection with the lens shape and proceed in a clockwise direction. 2) Advance the step angle for each point. 3) Calculate the new angle after step advancement. 4) Calculate the R-X coordinates.

Lower Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	15.676	6.41
55.831	27.699	-0.134
44.606	38.219	-8.892
33.382	**46.832**	**-19.531**
22.158	53.21	-31.643
10.933	57.108	-44.765
359.709	58.378	-58.395
348.485	56.97	-72.011
337.26	52.939	-85.092
326.036	46.438	-97.139
314.812	37.717	-107.69
303.587	27.109	-116.341
292.363	15.02	-122.762
281.139	1.913	-126.707
269.914	-11.712	-128.026
258.69	-25.333	-126.667
247.466	-38.429	-122.682
236.241	-50.499	-116.225
225.017	-61.081	-107.542
213.793	-69.771	-96.965
202.568	-76.235	-84.899
191.344	-80.227	-71.806
180.12	-81.594	-58.185
168.895	-80.284	-44.56
157.671	-76.347	-31.45
146.447	-69.933	-19.357
135.222	-61.288	-8.744
123.998	-50.742	-0.016
112.774	-38.699	6.491
101.549	-25.62	10.53
90.325	-12.005	11.946

Upper Loss of Synchronism Circle Coordinates		
Angle (degrees)	R	+ jX
67.055	-9.676	23.59
55.831	-21.699	30.134
44.606	-32.219	38.892
33.382	**-40.832**	**49.531**
22.158	-47.21	61.643
10.933	-51.108	74.765
359.709	-52.378	88.395
348.485	-50.97	102.011
337.26	-46.939	115.092
326.036	-40.438	127.139
314.812	-31.717	137.69
303.587	-21.109	146.341
292.363	-9.02	152.762
281.139	4.087	156.707
269.914	17.712	158.026
258.69	31.333	156.667
247.466	44.429	152.682
236.241	56.499	146.225
225.017	67.081	137.542
213.793	75.771	126.965
202.568	82.235	114.899
191.344	86.227	101.806
180.12	87.594	88.185
168.895	86.284	74.56
157.671	82.347	61.45
146.447	75.933	49.357
135.222	67.288	38.744
123.998	56.742	30.016
112.774	44.699	23.509
101.549	31.62	19.47
90.325	18.005	18.054

Figure 15i: Full tables of calculated lower and upper loss-of-synchronism circle coordinates. The highlighted row is the detailed calculated points in Figures 15d and 15h.

Application Specific to Criterion B

The PRC-026-1 – Attachment B, Criterion B evaluates overcurrent elements used for tripping. The same criteria as PRC-026-1 – Attachment B, Criterion A is used except for an additional criterion (No. 4) that calculates a current magnitude based upon generator internal voltage of 1.05 per unit. A value of 1.05 per unit generator voltage is used to establish a minimum pickup current value for overcurrent relays that have a time delay less than 15 cycles. The sending-end and receiving-end voltages are established at 1.05 per unit at 120 degree system separation angle. The 1.05 per unit is the typical upper end of the operating voltage, which is also consistent with the maximum power

transfer calculation using actual system source impedances in the PRC-023 NERC Reliability Standard. The formulas used to calculate the current are in Table 14 below.

Table 14: Example Calculation (Overcurrent)			
This example is for a 230 kV line terminal with a directional instantaneous phase overcurrent element set to 50 amps secondary times a CT ratio of 160:1 that equals 8,000 amps, primary. The following calculation is where V_S equals the base line-to-ground sending-end generator source voltage times 1.05 at an angle of 120 degrees, V_R equals the base line-to-ground receiving-end generator internal voltage times 1.05 at an angle of 0 degrees, and Z_{sys} equals the sum of the sending-end source, line, and receiving-end source impedances in ohms. Here, the instantaneous phase setting of 8,000 amps is greater than the calculated system current of 5,716 amps; therefore, it meets PRC-026-1 – Attachment B, Criterion B.			
Eq. (102)	$V_S = \frac{V_{LL}\angle 120°}{\sqrt{3}} \times 1.05$		
	$V_S = \frac{230{,}000\angle 120°\ V}{\sqrt{3}} \times 1.05$		
	$V_S = 139{,}430\angle 120°\ V$		
Receiving-end generator terminal voltage.			
Eq. (103)	$V_R = \frac{V_{LL}\angle 0°}{\sqrt{3}} \times 1.05$		
	$V_R = \frac{230{,}000\angle 0°\ V}{\sqrt{3}} \times 1.05$		
	$V_R = 139{,}430\angle 0°\ V$		
The total impedance of the system (Z_{sys}) equals the sum of the sending-end source impedance (Z_S), the impedance of the line (Z_L), and receiving-end impedance (Z_R) in ohms.			
Given:	$Z_S = 3 + j26\ \Omega$	$Z_L = 1.3 + j8.7\ \Omega$	$Z_R = 0.3 + j7.3\ \Omega$
Eq. (104)	$Z_{sys} = Z_S + Z_L + Z_R$		
	$Z_{sys} = (3 + j26)\ \Omega + (1.3 + j8.7)\ \Omega + (0.3 + j7.3)\ \Omega$		
	$Z_{sys} = 4.6 + j42\ \Omega$		
Total system current.			
Eq. (105)	$I_{sys} = \frac{(V_S - V_R)}{Z_{sys}}$		
	$I_{sys} = \frac{(139{,}430\angle 120°\ V - 139{,}430\angle 0°\ V)}{(4.6 + j42)\ \Omega}$		
	$I_{sys} = 5{,}715.82\angle 66.25°\ A$		

Application Specific to Three-Terminal Lines

If a three-terminal line is identified as an Element that is susceptible to a power swing based on Requirement R1, the load-responsive protective relays at each end of the three-terminal line must be evaluated.

As shown in Figure 15j, the source impedances at each end of the line can be obtained from the similar short circuit calculation as for the two-terminal line (assuming the parallel transfer impedances are ignored).

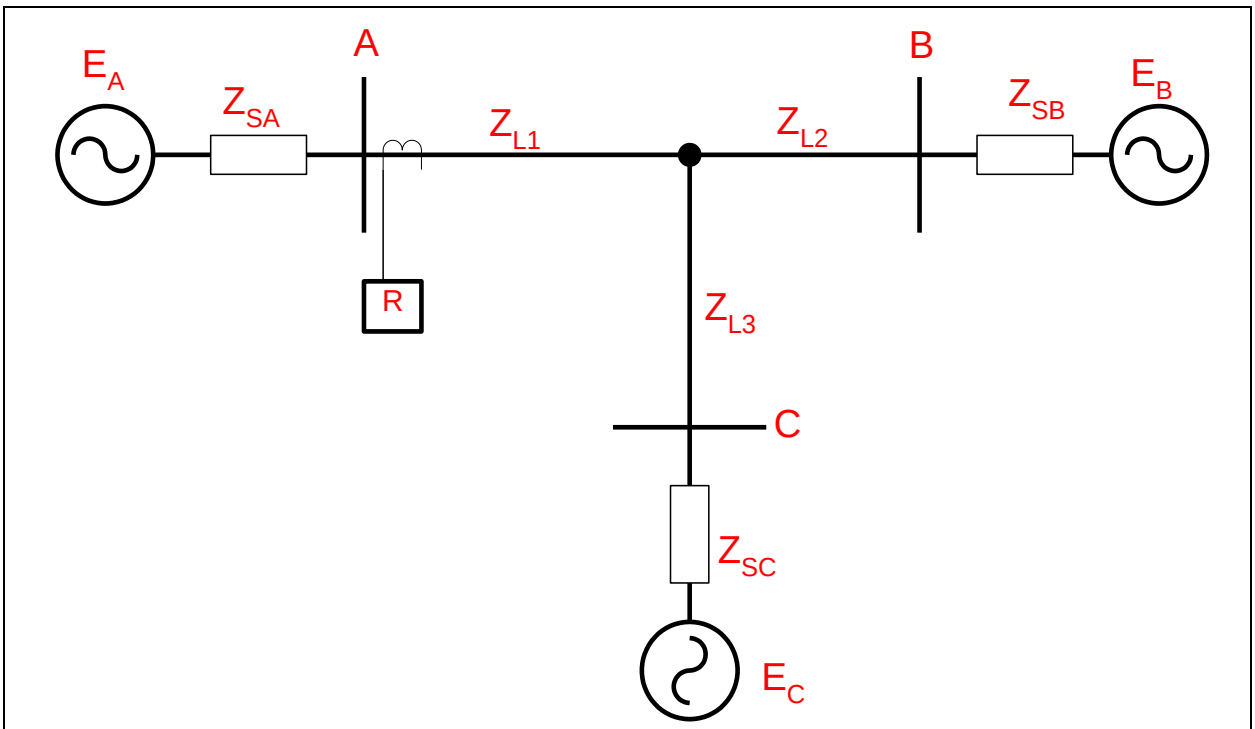


Figure 15j: Three-terminal line. To evaluate the load-responsive protective relays on the three-terminal line at Terminal A, the circuit in Figure 15j is first reduced to the equivalent circuit shown in Figure 15k. The evaluation process for the load-responsive protective relays on the line at Terminal A will now be the same as that of the two-terminal line.

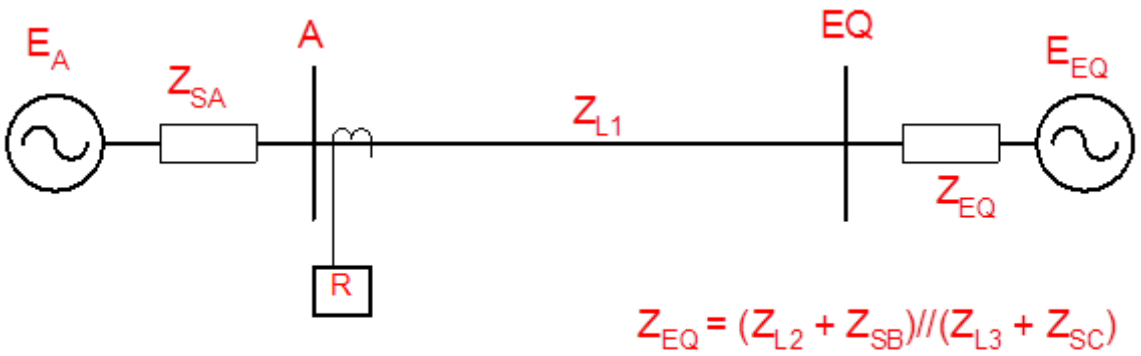


Figure 15k: Three-terminal line reduced to a two-terminal line.

Application to Generation Elements

As with transmission BES Elements, the determination of the apparent impedance seen at an Element located at, or near, a generation Facility is complex for power swings due to various interdependent quantities. These variances in quantities are caused by changes in machine internal voltage, speed governor action, voltage regulator action, the reaction of other local generators, and the reaction of other interconnected transmission BES Elements as the event progresses through the time domain. Though transient stability simulations may be used to determine the apparent impedance for verifying load-responsive relay settings,[19,20] Requirement R2, PRC-026-1 – Attachment B, Criteria A and B provides a simplified method for evaluating the load-responsive protective relay's susceptibility to tripping in response to a stable power swing without requiring stability simulations.

In general, the electrical center will be in the transmission system for cases where the generator is connected through a weak transmission system (high external impedance). In other cases where the generator is connected through a strong transmission system, the electrical center could be inside the unit connected zone.[21] In either case, load-responsive protective relays connected at the generator terminals or at the high-voltage side of the generator step-up (GSU) transformer may be challenged by power swings. Relays that may be challenged by power swings will be determined by the Planning Coordinator in Requirement R1 or by the Generator Owner after becoming aware of a generator, transformer, or transmission line BES Element that tripped[22] in response to a stable or unstable power swing due to the operation of its protective relay(s) in Requirement R2.

[19] Donald Reimert, *Protective Relaying for Power Generation Systems*, Boca Raton, FL, CRC Press, 2006.

[20] Prabha Kundur, *Power System Stability and Control*, EPRI, McGraw Hill, Inc., 1994.

[21] Ibid, Kundur.

[22] See Guidelines and Technical Basis section, "Becoming Aware of an Element That Tripped in Response to a Power Swing,"

Voltage controlled time-overcurrent and voltage-restrained time-overcurrent relays are excluded from this standard. When these relays are set based on equipment permissible overload capability, their operating times are much greater than 15 cycles for the current levels observed during a power swing.

Instantaneous overcurrent, time-overcurrent, and definite-time overcurrent relays with a time delay of less than 15 cycles for the current levels observed during a power swing are applicable and are required to be evaluated for identified Elements.

The generator loss-of-field protective function is provided by impedance relay(s) connected at the generator terminals. The settings are applied to protect the generator from a partial or complete loss of excitation under all generator loading conditions and, at the same time, be immune to tripping on stable power swings. It is more likely that the loss-of-field relay would operate during a power swing when the automatic voltage regulator (AVR) is in manual mode rather than when in automatic mode.[23] Figure 16 illustrates the loss-of-field relay in the R-X plot, which typically includes up to three zones of protection.

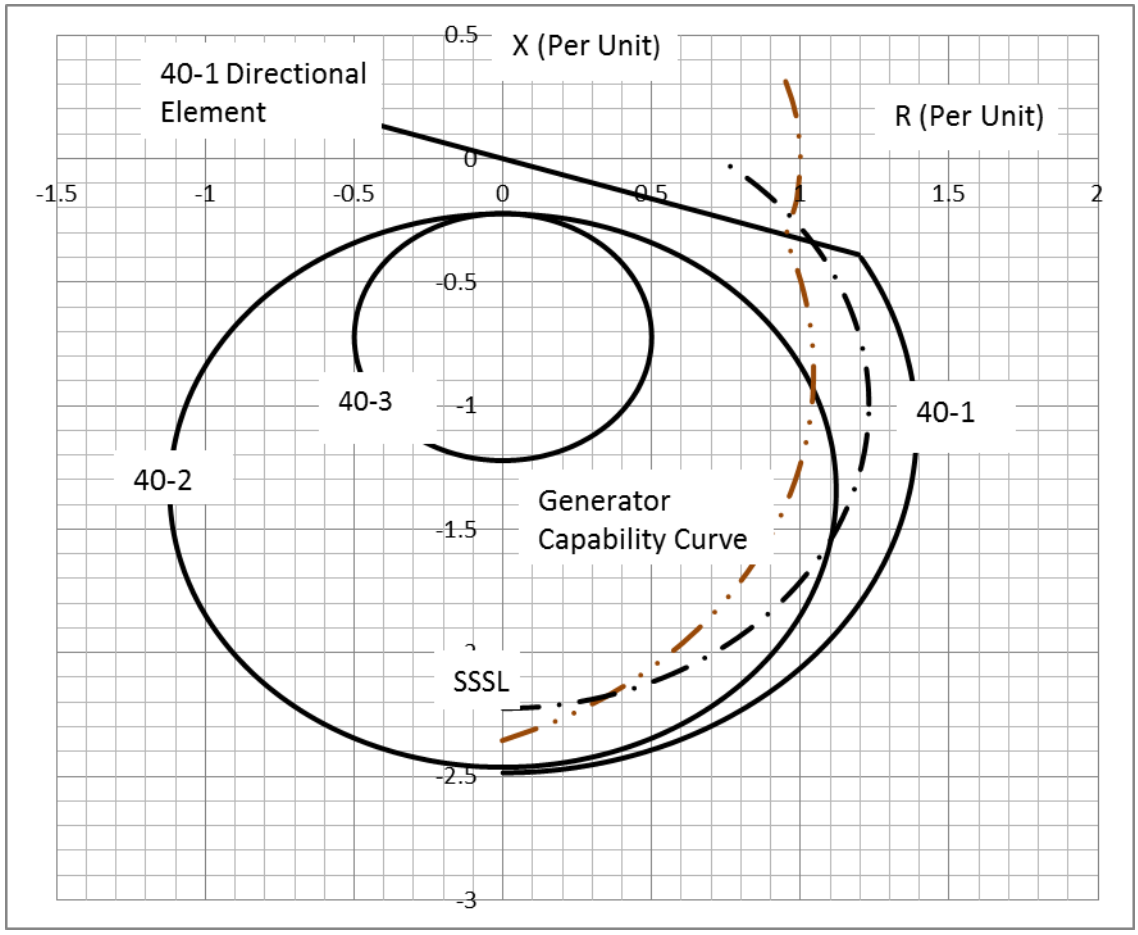


Figure 16: An R-X graph of typical impedance settings for loss-of-field relays.

[23] John Burdy, *Loss-of-excitation Protection for Synchronous Generators GER-3183*, General Electric Company.

Loss-of-field characteristic 40-1 has a wider impedance characteristic (positive offset) than characteristic 40-2 or characteristic 40-3 and provides additional generator protection for a partial loss of field or a loss of field under low load (less than 10% of rated). The tripping logic of this protection scheme is established by a directional contact, a voltage setpoint, and a time delay. The voltage and time delay add security to the relay operation for stable power swings. Characteristic 40-3 is less sensitive to power swings than characteristic 40-2 and is set outside the generator capability curve in the leading direction. Regardless of the relay impedance setting, PRC-019[24] requires that the "in-service limiters operate before Protection Systems to avoid unnecessary trip" and "in-service Protection System devices are set to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits." Time delays for tripping associated with loss-of-field relays[25,26] have a range from 15 cycles for characteristic 40-2 to 60 cycles for characteristic 40-1 to minimize tripping during stable power swings. In PRC-026-1, 15 cycles establishes a threshold for applicability; however, it is the responsibility of the Generator Owner to establish settings that provide security against stable power swings and, at the same time, dependable protection for the generator.

The simple two-machine system circuit (method also used in the Application to Transmission Elements section) is used to analyze the effect of a power swing at a generator facility for load-responsive relays. In this section, the calculation method is used for calculating the impedance seen by the relay connected at a point in the circuit.[27] The electrical quantities used to determine the apparent impedance plot using this method are generator saturated transient reactance (X'_d), GSU transformer impedance (X_{GSU}), transmission line impedance (Z_L), and the system equivalent (Z_e) at the point of interconnection. All impedance values are known to the Generator Owner except for the system equivalent. The system equivalent is obtainable from the Transmission Owner. The sending-end and receiving-end source voltages are varied from 0.0 to 1.0 per unit to form the lens shape portion of the unstable power swing region. The voltage range of 0.7 to 1.0 results in a ratio range from 0.7 to 1.43. This ratio range is used to form the lower and upper loss-of-synchronism circle shapes of the unstable power swing region. A system separation angle of 120 degrees is used in accordance with PRC-026-1 – Attachment B criteria for each load-responsive protective relay evaluation.

Table 15 below is an example calculation of the apparent impedance locus method based on Figures 17 and 18.[28] In this example, the generator is connected to the 345 kV transmission system through the GSU transformer and has the listed ratings. Note that the load-responsive protective relays in this example may have ownership with the Generator Owner or the Transmission Owner.

[24] Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

[25] Ibid, Burdy.

[26] *Applied Protective Relaying*, Westinghouse Electric Corporation, 1979.

[27] Edward Wilson Kimbark, *Power System Stability, Volume II: Power Circuit Breakers and Protective Relays*, Published by John Wiley and Sons, 1950.

[28] Ibid, Kimbark.

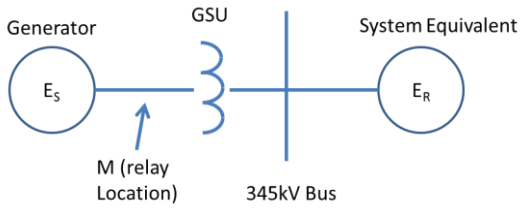


Figure 17: Simple one-line diagram of the system to be evaluated.

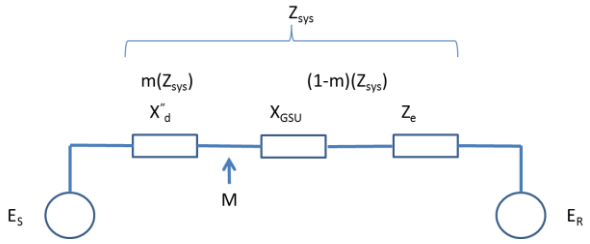


Figure 18: Simple system equivalent impedance diagram to be evaluated.[29]

Table15: Example Data (Generator)	
Input Descriptions	**Input Values**
Synchronous Generator nameplate (MVA)	940 MVA
Saturated transient reactance (940 MVA base)	$X'_d = 0.3845$ per unit
Generator rated voltage (Line-to-Line)	20 kV
Generator step-up (GSU) transformer rating	880 MVA
GSU transformer reactance (880 MVA base)	$X_{GSU} = 16.05\%$
System Equivalent (100 MVA base)	$Z_e = 0.00723\angle 90°$ per unit
Generator Owner Load-Responsive Protective Relays	
40-1	Positive Offset Impedance
	Offset = 0.294 per unit
	Diameter = 0.294 per unit
40-2	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 2.24 per unit
40-3	Negative Offset Impedance
	Offset = 0.22 per unit
	Diameter = 1.00 per unit
21-1	Diameter = 0.643 per unit
	MTA = 85°

[29] Ibid, Kimbark.

Table15: Example Data (Generator)	
50	I (pickup) = 5.0 per unit
Transmission Owned Load-Responsive Protective Relays	
21-2	Diameter = 0.55 per unit
	MTA = 85°

Calculations shown for a 120 degree angle and $E_S/E_R = 1$. The equation for calculating Z_R is:[30]

Eq. (106) $$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$$

Where m is the relay location as a function of the total impedance (real number less than 1)

E_S and E_R is the sending-end and receiving-end voltages

Z_{sys} is the total system impedance

Z_R is the complex impedance at the relay location and plotted on an R-X diagram

All of the above are constants (940 MVA base) while the angle δ is varied. Table 16 below contains calculations for a generator using the data listed in Table 15.

Table16: Example Calculations (Generator)			
The following calculations are on a 940 MVA base.			
Given:	$X'_d = j0.3845\ pu$	$X_{GSU} = j0.17144\ pu$	$Z_e = j0.06796\ pu$
Eq. (107)	$Z_{sys} = X'_d + X_{GSU} + Z_e$		
	$Z_{sys} = j0.3845\ pu + j0.17144\ pu + j0.06796\ pu$		
	$Z_{sys} = 0.6239\ \angle 90°\ pu$		
Eq. (108)	$m = \frac{X'_d}{Z_{sys}} = \frac{0.3845}{0.6239} = 0.6163$		
Eq. (109)	$Z_R = \left(\frac{(1-m)(E_S\angle\delta) + (m)(E_R)}{E_S\angle\delta - E_R}\right) \times Z_{sys}$		
	$Z_R = \left(\frac{(1-0.6163) \times (1\angle 120°) + (0.6163)(1\angle 0°)}{1\angle 120° - 1\angle 0°}\right) \times (0.6239\angle 90°)\ pu$		

[30] Ibid, Kimbark.

Table16: Example Calculations (Generator)	
	$Z_R = \left(\frac{0.4244 + j0.3323}{-1.5 + j\ 0.866}\right) \times (0.6239\angle 90°)\ pu$
	$Z_R = (0.3116 \angle -111.95°) \times (0.6239\angle 90°)\ pu$
	$Z_R = 0.194 \angle -21.95°\ pu$
	$Z_R = -0.18 - j0.073\ pu$

Table 17 lists the swing impedance values at other angles and at E_S/E_R = 1, 1.43, and 0.7. The impedance values are plotted on an R-X graph with the center being at the generator terminals for use in evaluating impedance relay settings.

Table 17: Sample Calculations for a Swing Impedance Chart for Varying Voltages at the Sending-End and Receiving-End.

	E_S/E_R=1		E_S/E_R=1.43		E_S/E_R=0.7	
	Z_R		Z_R		Z_R	
Angle (δ) (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)	Magnitude (pu)	Angle (Degrees)
90	0.320	-13.1	0.296	6.3	0.344	-31.5
120	0.194	-21.9	0.173	-0.4	0.227	-40.1
150	0.111	-41.0	0.082	-10.3	0.154	-58.4
210	0.111	-25.9	0.082	190.3	0.154	238.4
240	0.194	201.9	0.173	180.4	0.225	220.1
270	0.320	193.1	0.296	173.7	0.344	211.5

Requirement R2 Generator Examples

Distance Relay Application

Based on PRC-026-1 – Attachment B, Criterion A, the distance relay (21-1) (i.e., owned by the Generation Owner) characteristic is in the region where a stable power swing would not occur as shown in Figure 19. There is no further obligation to the owner in this standard for this load-responsive protective relay.

The distance relay (21-2) (i.e., owned by the Transmission Owner) is connected at the high-voltage side of the GSU transformer and its impedance characteristic is in the region where a stable power swing could occur causing the relay to operate. In this example, if the intentional time delay of this relay is less than 15 cycles, the PRC-026 – Attachment B, Criterion A cannot be met, thus the Transmission Owner is required to create a CAP (Requirement R3). Some of the options include,

but are not limited to, changing the relay setting (i.e., impedance reach, angle, time delay), modify the scheme (i.e., add PSB), or replace the Protection System. Note that the relay may be excluded from this standard if it has an intentional time delay equal to or greater than 15 cycles.

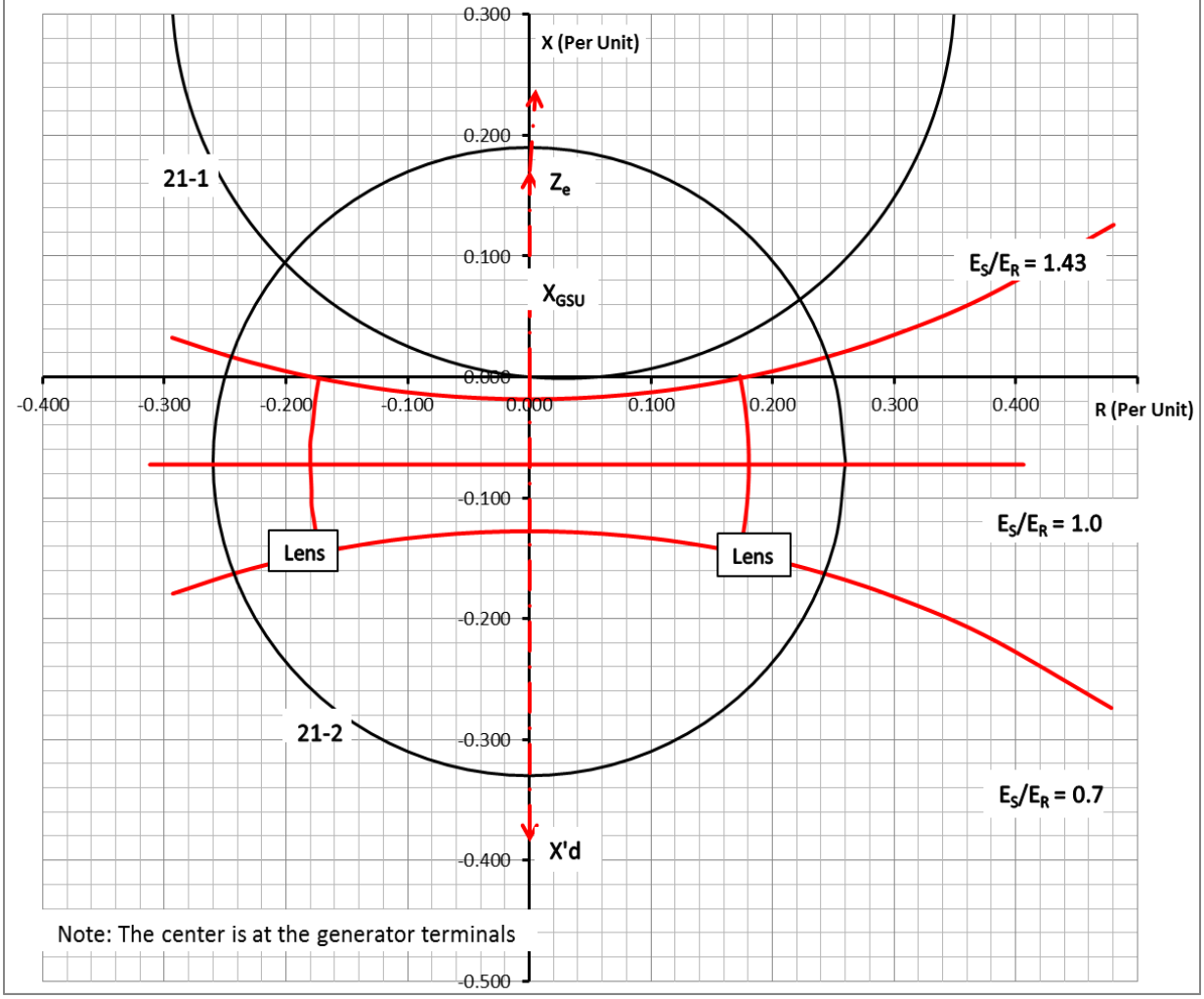


Figure 19: Swing impedance graph for impedance relays at a generating facility.

Loss-of-Field Relay Application

In Figure 20, the R-X diagram shows the loss-of-field relay (40-1 and 40-2) characteristics are in the region where a stable power swing can cause a relay operation. Protective relay 40-1 would be excluded if it has an intentional time delay equal to or greater than 15 cycles. Similarly, 40-2 would be excluded if its intentional time delay is equal to or greater than 15 cycles. For example, if 40-1 has a time delay of 1 second and 40-2 has a time delay of 0.25 seconds, they are excluded and there is no further obligation on the Generator Owner in this standard for these relays. The

loss-of-field relay characteristic 40-3 is entirely inside the unstable power swing region. In this case, the owner may select high speed tripping on operation of the 40-3 impedance element.

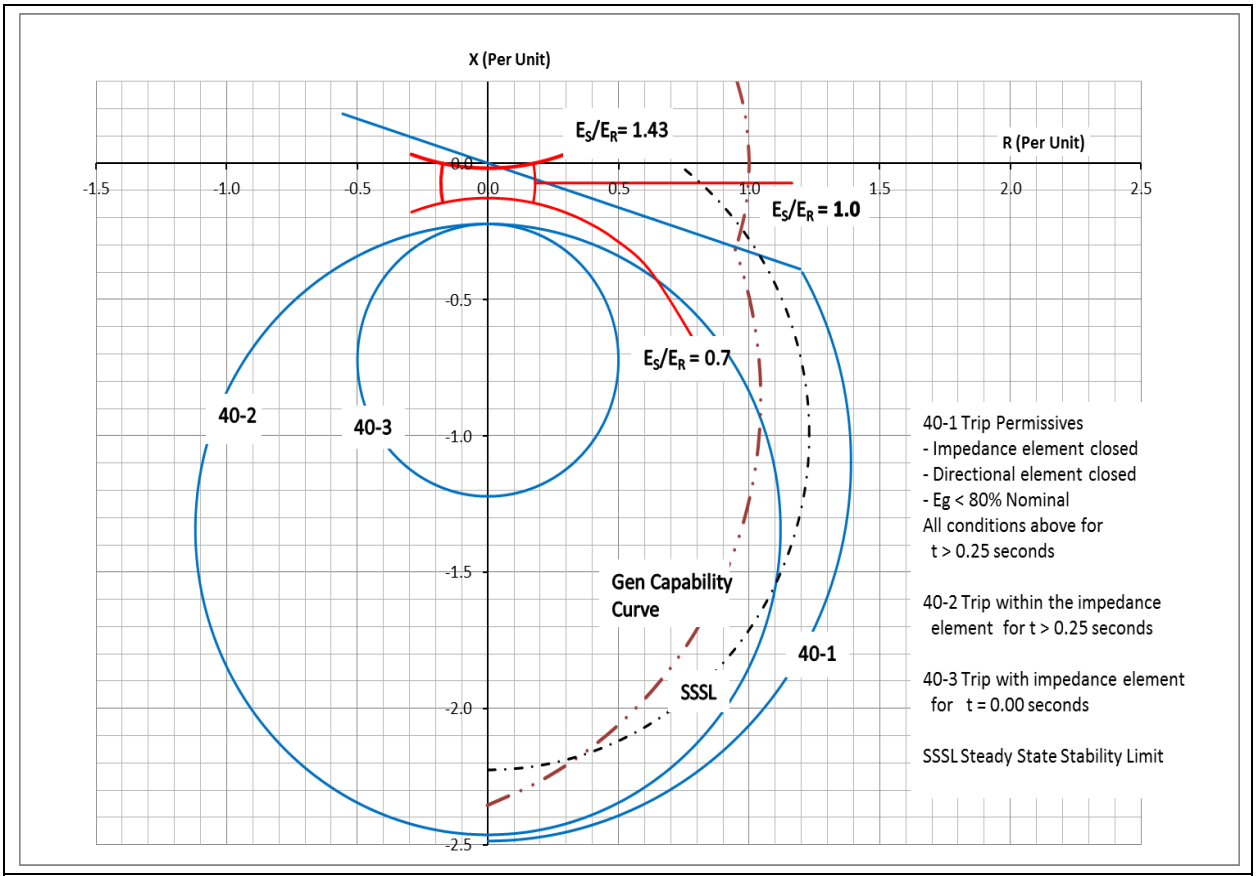


Figure 20: Typical R-X graph for loss-of-field relays with a portion of the unstable power swing region defined by PRC-026-1 – Attachment B, Criterion A.

Instantaneous Overcurrent Relay

In similar fashion to the transmission line overcurrent example calculation in Table 14, the instantaneous overcurrent relay minimum setting is established by PRC-026-1 – Attachment B, Criterion B. The solution is found by:

Eq. (110) $$I_{sys} = \frac{E_S - E_R}{Z_{\text{sys}}}$$

As stated in the relay settings in Table 15, the relay is installed on the high-voltage side of the GSU transformer with a pickup of 5.0 per unit. The maximum allowable current is calculated below.

$$I_{sys} = \frac{(1.05\angle 120° - 1.05\angle 0°)}{0.6239\angle 90°}\ pu$$

$$I_{sys} = \frac{1.819\angle 150°}{0.6239\angle 90°} pu$$

$$I_{sys} = 2.91\ \angle 60°\ pu$$

The instantaneous phase setting of 5.0 per unit is greater than the calculated system current of 2.91 per unit; therefore, it meets the PRC-026-1 – Attachment B, Criterion B.

Out-of-Step Tripping for Generation Facilities

Out-of-step protection for the generator generally falls into three different schemes. The first scheme is a distance relay connected at the high-voltage side of the GSU transformer with the directional element looking toward the generator. Because this relay setting may be the same setting used for generator backup protection (see Requirement R2 Generator Examples, Distance Relay Application), it is susceptible to tripping in response to stable power swings and would require modification. Because this scheme is susceptible to tripping in response to stable power swings and any modification to the mho circle will jeopardize the overall protection of the out-of-step protection of the generator, available technical literature does not recommend using this scheme specifically for generator out-of-step protection. The second and third out-of-step Protection System schemes are commonly referred to as single and double blinder schemes. These schemes are installed or enabled for out-of-step protection using a combination of blinders, a mho element, and timers. The combination of these protective relay functions provides out-of-step protection and discrimination logic for stable and unstable power swings. Single blinder schemes use logic that discriminate between stable and unstable power swings by issuing a trip command after the first slip cycle. Double blinder schemes are more complex than the single blinder scheme and, depending on the settings of the inner blinder, a trip for a stable power swing may occur. While the logic discriminates between stable and unstable power swings in either scheme, it is important that the trip initiating blinders be set at an angle greater than the stability limit of 120 degrees to remove the possibility of a trip for a stable power swing. Below is a discussion of the double blinder scheme.

Double Blinder Scheme

The double blinder scheme is a method for measuring the rate of change of positive sequence impedance for out-of-step swing detection. The scheme compares a timer setting to the actual elapsed time required by the impedance locus to pass between two impedance characteristics. In this case, the two impedance characteristics are simple blinders, each set to a specific resistive reach on the R-X plane. Typically, the two blinders on the left half plane are the mirror images of those on the right half plane. The scheme typically includes a mho characteristic which acts as a starting element, but is not a tripping element.

The scheme detects the blinder crossings and time delays as represented on the R-X plane as shown in Figure 21. The system impedance is composed of the generator transient (X_d'), GSU transformer (X_T), and transmission system (X_{system}), impedances.

The scheme logic is initiated when the swing locus crosses the outer Blinder R1 (Figure 21), on the right at separation angle α. The scheme only commits to take action when a swing crosses the

inner blinder. At this point the scheme logic seals in the out-of-step trip logic at separation angle β. Tripping actually asserts as the impedance locus leaves the scheme characteristic at separation angle δ.

The power swing may leave both inner and outer blinders in either direction, and tripping will assert. Therefore, the inner blinder must be set such that the separation angle β is large enough that the system cannot recover. This angle should be set at 120 degrees or more. Setting the angle greater than 120 degrees satisfies the PRC-026-1 – Attachment B, Criterion A (No. 1, 1st bullet) since the tripping function is asserted by the blinder element. Transient stability studies may indicate that a smaller stability limit angle is acceptable under PRC-026-1 – Attachment B, Criterion A (No. 1, 2nd bullet). In this respect, the double blinder scheme is similar to the double lens and triple lens schemes and many transmission application out-of-step schemes.

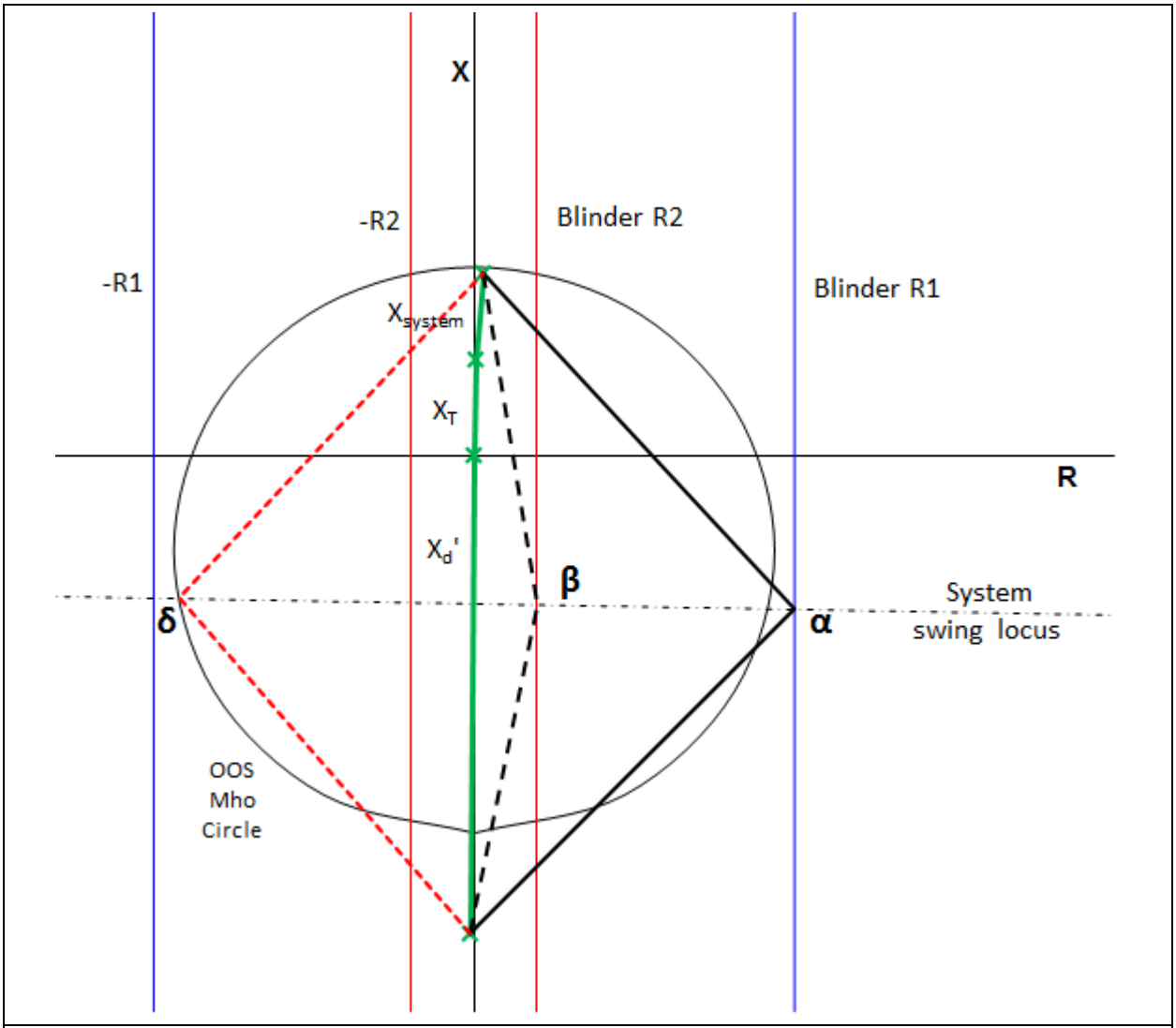


Figure 21: Double Blinder Scheme generic out of step characteristics.

Figure 22 illustrates a sample setting of the double blinder scheme for the example 940 MVA generator. The only setting requirement for this relay scheme is the right inner blinder, which must be set greater than the separation angle of 120 degrees (or a lesser angle based on a transient stability study) to ensure that the out-of-step protective function is expected to not trip in response to a stable power swing during non-Fault conditions. Other settings such as the mho characteristic, outer blinders, and timers are set according to transient stability studies and are not a part of this standard.

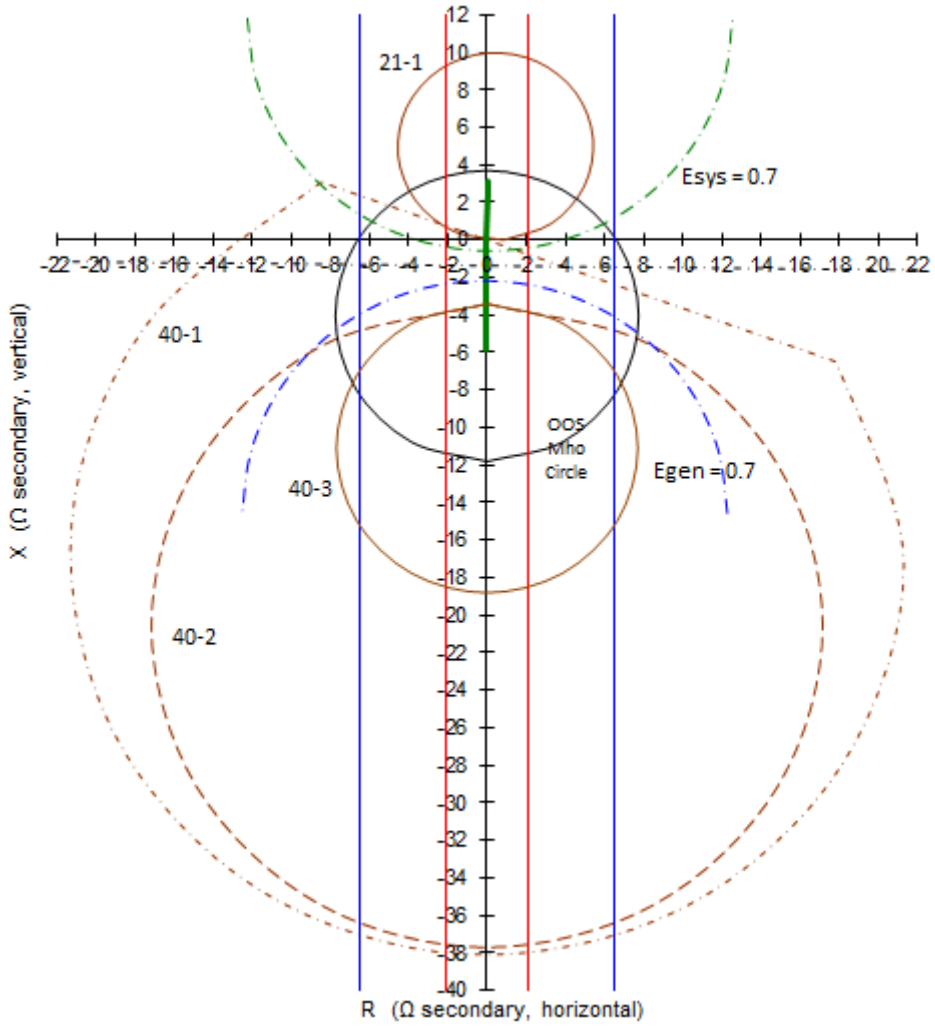


Figure 22: Double Blinder Out-of-Step Scheme with unit impedance data and load-responsive protective relay impedance characteristics for the example 940 MVA generator, scaled in relay secondary ohms.

Requirement R3

To achieve the stated purpose of this standard, which is to ensure that relays are expected to not trip in response to stable power swings during non-Fault conditions, this Requirement ensures that the applicable entity develops a Corrective Action Plan (CAP) that reduces the risk of relays tripping in response to a stable power swing during non-Fault conditions that may occur on any applicable BES Element.

Requirement R4

To achieve the stated purpose of this standard, which is to ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions, the applicable entity is required to implement any CAP developed pursuant to Requirement R3 such that the Protection System will meet PRC-026-1 – Attachment B criteria or can be excluded under the PRC-026-1 – Attachment A criteria (e.g., modifying the Protection System so that relay functions are supervised by power swing blocking or using relay systems that are immune to power swings), while maintaining dependable fault detection and dependable out-of-step tripping (if out-of-step tripping is applied at the terminal of the BES Element). Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until all actions are complete. Accomplishing this objective is intended to reduce the occurrence of Protection System tripping during a stable power swing, thereby improving reliability and minimizing risk to the BES.

The following are examples of actions taken to complete CAPs for a relay that did not meet PRC-026-1 – Attachment B and could be at-risk of tripping in response to a stable power swing during non-Fault conditions. A Protection System change was determined to be acceptable (without diminishing the ability of the relay to protect for faults within its zone of protection).

> **Example R4a:** Actions: Settings were issued on 6/02/2015 to reduce the Zone 2 reach of the impedance relay used in the directional comparison unblocking (DCUB) scheme from 30 ohms to 25 ohms so that the relay characteristic is completely contained within the lens characteristic identified by the criterion. The settings were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.
>
> **Example R4b:** Actions: Settings were issued on 6/02/2015 to enable out-of-step blocking on the existing microprocessor-based relay to prevent tripping in response to stable power swings. The setting changes were applied to the relay on 6/25/2015. CAP was completed on 06/25/2015.

The following is an example of actions taken to complete a CAP for a relay responding to a stable power swing that required the addition of an electromechanical power swing blocking relay.

> **Example R4c:** Actions: A project for the addition of an electromechanical power swing blocking relay to supervise the Zone 2 impedance relay was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The relay installation was completed on 9/25/2015. CAP was completed on 9/25/2015.

The following is an example of actions taken to complete a CAP with a timetable that required updating for the replacement of the relay.

> **Example R4d:** Actions: A project for the replacement of the impedance relays at both terminals of line X with line current differential relays was initiated on 6/5/2015 to prevent tripping in response to stable power swings. The completion of the project was postponed due to line outage rescheduling from 11/15/2015 to 3/15/2016. Following the timetable change, the impedance relay replacement was completed on 3/18/2016. CAP was completed on 3/18/2016.

The CAP is complete when all the documented actions to remedy the specific problem (i.e., unnecessary tripping during stable power swings) are completed.

Justification for Including Unstable Power Swings in the Requirements

Protection Systems that are applicable to the Standard and must be secure for a stable power swing condition (i.e., meets PRC-026-1 – Attachment B criteria) are identified based on Elements that are susceptible to both stable and unstable power swings. This section provides an example of why Elements that trip in response to unstable power swings (in addition to stable power swings) are identified and that their load-responsive protective relays need to be evaluated under PRC-026-1 – Attachment B criteria.

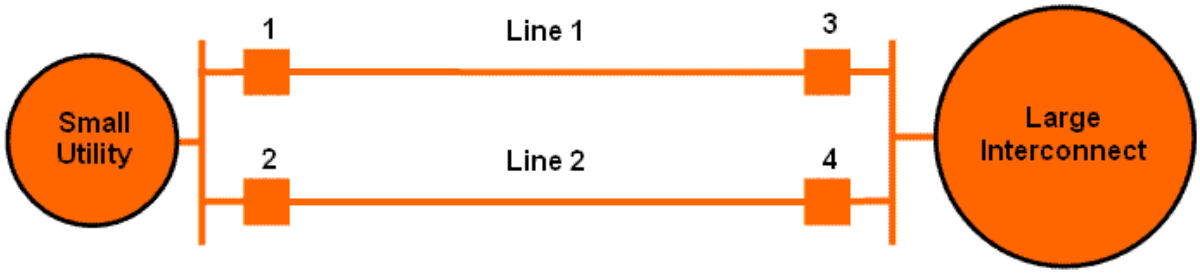


Figure 23: A simple electrical system where two lines tie a small utility to a much larger interconnection.

In Figure 23 the relays at circuit breakers 1, 2, 3, and 4 are equipped with a typical overreaching Zone 2 pilot system, using a Directional Comparison Blocking (DCB) scheme. Internal faults (or power swings) will result in instantaneous tripping of the Zone 2 relays if the measured fault or power swing impedance falls within the zone 2 operating characteristic. These lines will trip on

pilot Zone 2 for out-of-step conditions if the power swing impedance characteristic enters into Zone 2. All breakers are rated for out-of-phase switching.

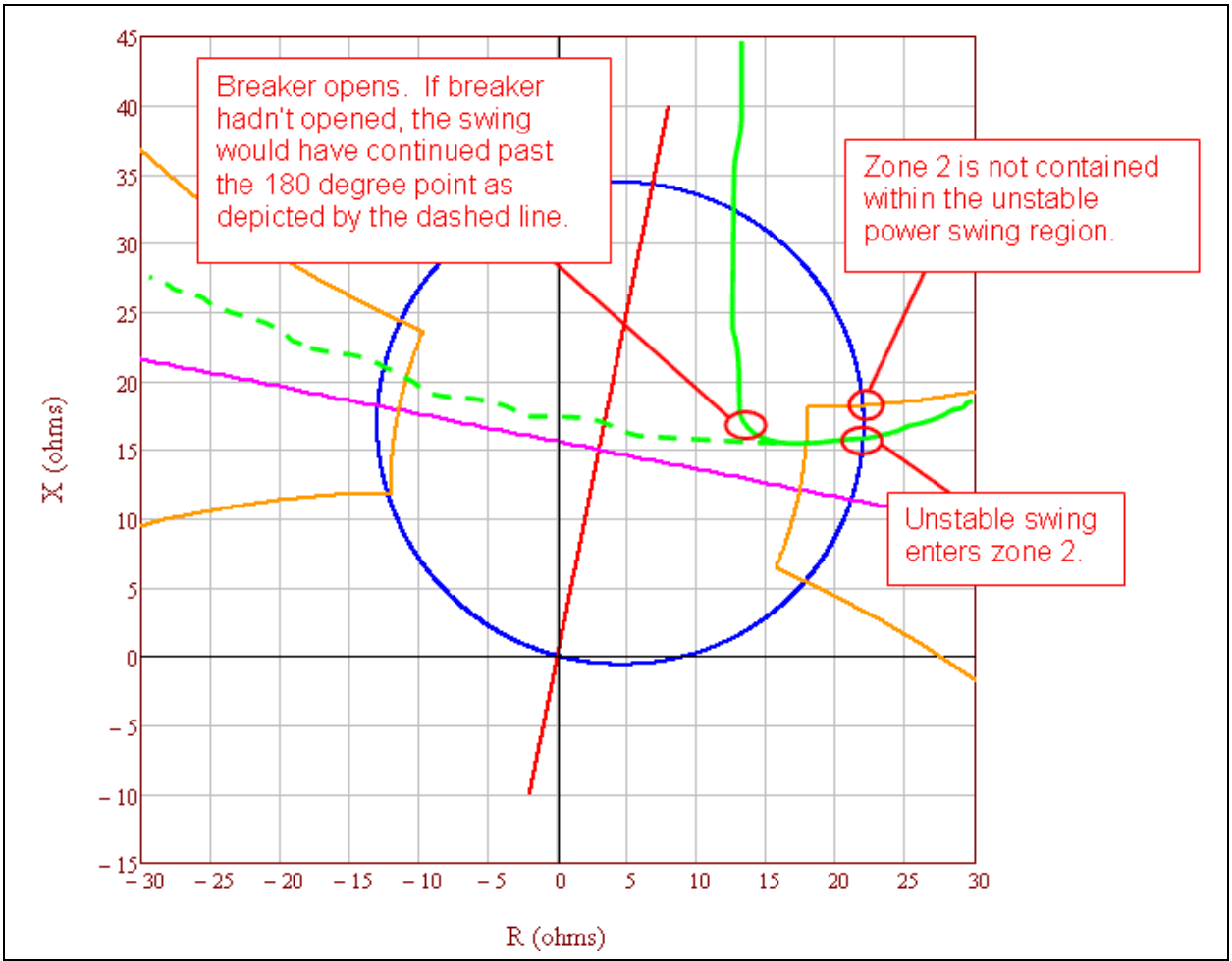


Figure 24: In this case, the Zone 2 element on circuit breakers 1, 2, 3, and 4 did not meet the PRC-026-1 – Attachment B criteria (this figure depicts the power swing as seen by relays on breakers 3 and 4).

In Figure 24, a large disturbance occurs within the small utility and its system goes out-of-step with the large interconnect. The small utility is importing power at the time of the disturbance. The actual power swing, as shown by the solid green line, enters the Zone 2 relay characteristic on the terminals of Lines 1, 2, 3, and 4 causing both lines to trip as shown in Figure 25.

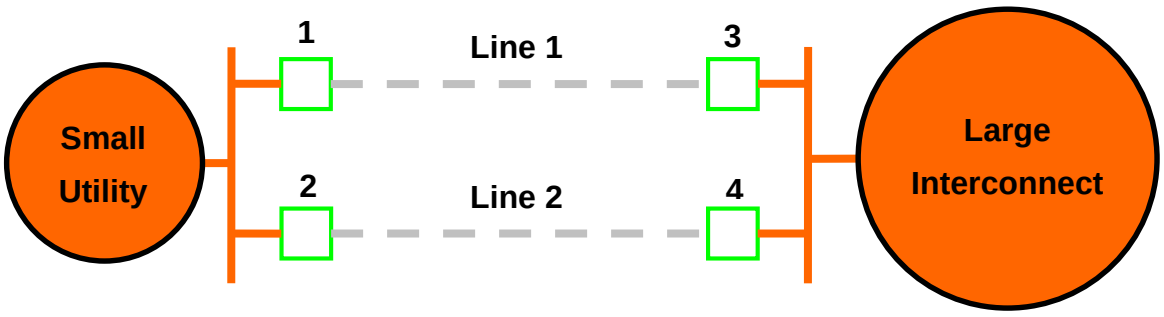


Figure 25: Islanding of the small utility due to Lines 1 and 2 tripping in response to an unstable power swing.

In Figure 25, the relays at circuit breakers 1, 2, 3, and 4 have correctly tripped due to the unstable power swing (shown by the dashed green line in Figure 24), de-energizing Lines 1 and 2, and creating an island between the small utility and the big interconnect. The small utility shed 500 MW of load on underfrequency and maintained a load to generation balance.

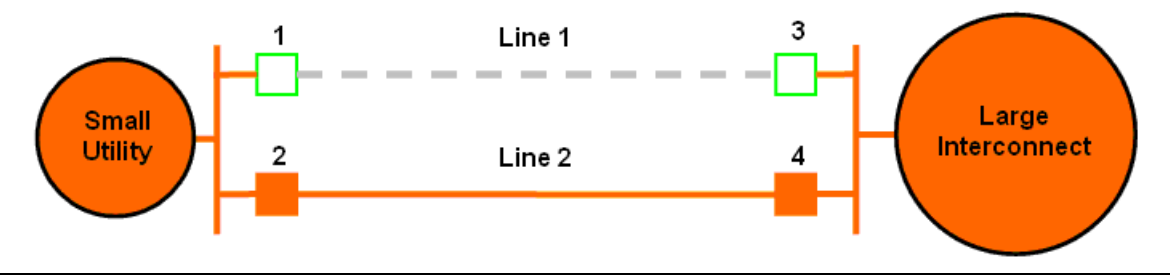


Figure 26: Line 1 is out-of-service for maintenance, Line 2 is loaded beyond its normal rating (but within its emergency rating).

Subsequent to the correct tripping of Lines 1 and 2 for the unstable power swing in Figure 25, another system disturbance occurs while the system is operating with Line 1 out-of-service for maintenance. The disturbance causes a stable power swing on Line 2, which challenges the relays at circuit breakers 2 and 4 as shown in Figure 27.

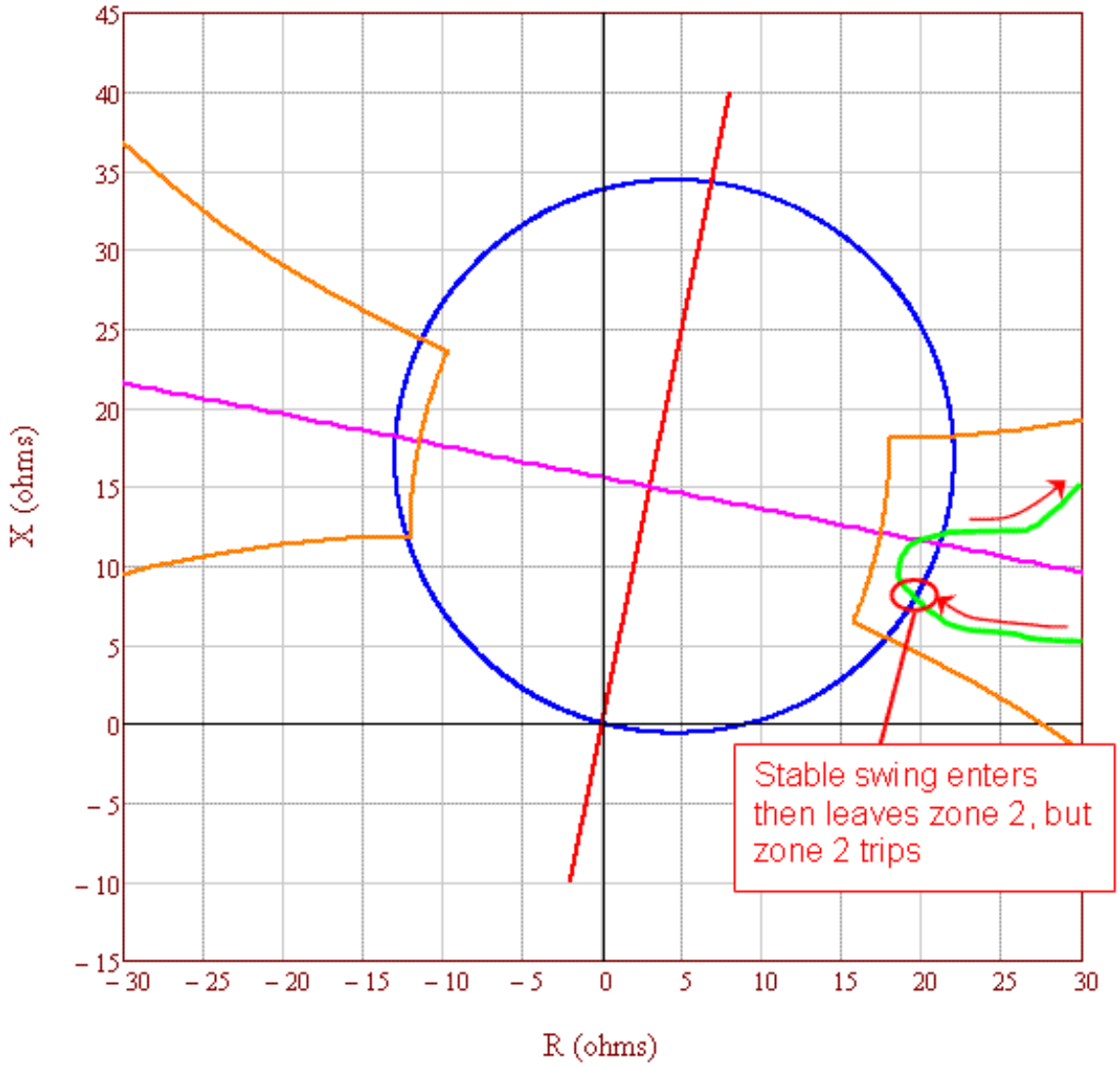


Figure 27: Relays on circuit breakers 2 and 4 were not addressed to meet the PRC-026-1 – Attachment B criteria following the previous unstable power swing event.

If the relays on circuit breakers 2 and 4 were not addressed under the Requirements for the previous unstable power swing condition, the relays would trip in response to the stable power swing, which would result in unnecessary system separation, load shedding, and possibly cascading or blackout.

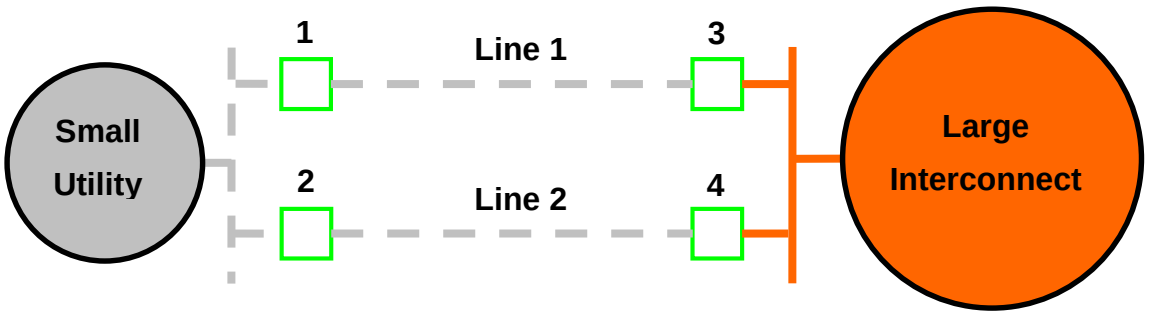


Figure 28: Possible blackout of the small utility.

If the relays that tripped in response to the previous unstable power swing condition in Figure 24 were addressed under the Requirements to meet PRC-026-1 - Attachment B criteria, the unnecessary tripping of the relays for the stable power swing shown in Figure 28 would have been averted, and the possible blackout of the small utility would have been avoided.

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

The Planning Coordinator has a wide-area view and is in the position to identify generator, transformer, and transmission line BES Elements which meet the criteria, if any. The criteria-based approach is consistent with the NERC System Protection and Control Subcommittee (SPCS) technical document *Protection System Response to Power Swings*, August 2013 ("PSRPS Report"),[31] which recommends a focused approach to determine an at-risk BES Element. See the Guidelines and Technical Basis for a detailed discussion of the criteria.

Rationale for R2

The Generator Owner and Transmission Owner are in a position to determine whether their load-responsive protective relays meet the PRC-026-1 – Attachment B criteria. Generator, transformer, and transmission line BES Elements are identified by the Planning Coordinator in Requirement R1 and by the Generator Owner and Transmission Owner following an actual event where the Generator Owner and Transmission Owner became aware (i.e., through an event analysis or

[31] NERC System Protection and Control Subcommittee, *Protection System Response to Power Swings*, August 2013: http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf)

Protection System review) tripping was due to a stable or unstable power swing. A period of 12 calendar months allows sufficient time for the entity to conduct the evaluation.

Rationale for R3

To meet the reliability purpose of the standard, a CAP is necessary to ensure the entity's Protection System meets the PRC-026-1 – Attachment B criteria (1st bullet) so that protective relays are expected to not trip in response to stable power swings. A CAP may also be developed to modify the Protection System for exclusion under PRC-026-1 – Attachment A (2nd bullet). Such an exclusion will allow the Protection System to be exempt from the Requirement for future events. The phrase, "…while maintaining dependable fault detection and dependable out-of-step tripping…" in Requirement R3 describes that the entity is to comply with this standard, while achieving their desired protection goals. Refer to the Guidelines and Technical Basis, Introduction, for more information.

Rationale for R4

Implementation of the CAP must accomplish all identified actions to be complete to achieve the desired reliability goal. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting CAP changes and completion of activities provides measurable progress and confirmation of completion.

Rationale for Attachment B (Criterion A)

The PRC-026-1 – Attachment B, Criterion A provides a basis for determining if the relays are expected to not trip for a stable power swing having a system separation angle of up to 120 degrees with the sending-end and receiving-end voltages varying from 0.7 to 1.0 per unit (See Guidelines and Technical Basis).

*** FOR INFORMATIONAL PURPOSES ONLY ***

Enforcement Dates: Standard PRC-026-1 — Relay Performance During Stable Power Swings

United States

Standard	Requirement	Enforcement Date	Inactive Date
PRC-026-1	R2.	01/01/2020	
PRC-026-1	R4.	01/01/2020	
PRC-026-1	R1.	01/01/2018	
PRC-026-1	2.1.	01/01/2020	
PRC-026-1	2.2.	01/01/2020	
PRC-026-1	R3.	01/01/2020	

Printed On: May 12, 2016, 11:07 AM

Exhibit B: List of Currently Effective NERC Reliability Standards

Resource and Demand Balancing (BAL)	
BAL-001-1	Real Power Balancing Control Performance
BAL-001-TRE-1	Primary Frequency Response in the ERCOT Region
BAL-002-1	Disturbance Control Performance
BAL-002-WECC-2	Contingency Reserve
BAL-003-1.1	Frequency Response and Frequency Bias Setting
BAL-004-0	Time Error Correction
BAL-004-WECC-02	Automatic Time Error Correction (ATEC)
BAL-005-0.2b	Automatic Generation Control
BAL-006-2	Inadvertent Interchange
BAL-502-RFC-02	Planning Resource Adequacy Analysis, Assessment and Documentation
Communications (COM)	
COM-001-1.1	Telecommunications
COM-001-2.1	Communications
COM-002-2	Communications and Coordination
Critical Infrastructure Protection (CIP)	
CIP-002-3	Cyber Security — Critical Cyber Asset Identification
CIP-003-3	Cyber Security — Security Management Controls
CIP-004-3a	Cyber Security — Personnel & Training
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets
CIP-007-3a	Cyber Security — Systems Security Management
CIP-008-3	Cyber Security — Incident Reporting and Response Planning
CIP-009-3	Cyber Security — Recovery Plans for Critical Cyber Assets
CIP-014-2	Physical Security
Emergency Preparedness and Operations (EOP)	
EOP-001-2.1b	Emergency Operations Planning
EOP-002-3.1	Capacity and Energy Emergencies
EOP-003-2	Load Shedding Plans
EOP-004-2	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
Facilities Design, Connections, and Maintenance (FAC)	
FAC-001-2	Facility Interconnection Requirements
FAC-002-2	Facility Interconnection Studies
FAC-003-3	Transmission Vegetation Management
FAC-008-3	Facility Ratings
FAC-010-2.1	System Operating Limits Methodology for the Planning Horizon
FAC-011-2	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-1	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
INT-011-1.1	Intra-Balancing Authority Transaction Identification
Interconnection Reliability Operations and Coordination (IRO)	
IRO-001-1.1	Reliability Coordination — Responsibilities and Authorities
IRO-002-2	Reliability Coordination — Facilities
IRO-003-2	Reliability Coordination — Wide-Area View
IRO-004-2	Reliability Coordination — Operations Planning
IRO-005-3.1a	Reliability Coordination — Current Day Operations
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-008-1	Reliability Coordinator Operational Analyses and Real-time Assessments
IRO-009-2	Reliability Coordinator Actions to Operate Within IROLs
IRO-010-1a	Reliability Coordinator Data Specification and Collection
IRO-014-1	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators
IRO-015-1	Notifications and Information Exchange Between Reliability Coordinators
IRO-016-1	Coordination of Real-time Activities Between Reliability Coordinators

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-010-0	Steady-State Data for Modeling and Simulation of the Interconnected Transmission System
MOD-012-0	Dynamics Data for Modeling and Simulation of the Interconnected Transmission System
MOD-016-1.1	Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, and Controllable Demand-Side Management
MOD-017-0.1	Aggregated Actual and Forecast Demands and Net Energy for Load
MOD-018-0	Treatment of Nonmember Demand Data and How Uncertainties are Addressed in the Forecasts of Demand and Net Energy for Load
MOD-019-0.1	Reporting of Interruptible Demands and Direct Control Load Management
MOD-020-0	Providing Interruptible Demands and Direct Control Load Management Data to System Operators and Reliability Coordinators
MOD-021-1	Documentation of the Accounting Methodology for the Effects of Demand-Side Management in Demand and Energy Forecasts
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-029-1a	Rated System Path Methodology
MOD-030-2	Flowgate Methodology
MOD-032-1	Data for Power System Modeling and Analysis
Nuclear (NUC)	
NUC-001-3	Nuclear Plant Interface Coordination
Personnel Performance, Training, and Qualifications (PER)	
PER-001-0.2	Operating Personnel Responsibility and Authority
PER-003-1	Operating Personnel Credentials
PER-004-2	Reliability Coordination — Staffing
PER-005-1	System Personnel Training
Protection and Control (PRC)	
PRC-001-1.1(ii)	System Protection Coordination
PRC-002-NPCC-01	Disturbance Monitoring
PRC-004-2.1(i)a	Analysis and Mitigation of Transmission and Generation Protection System Misoperations
PRC-004-WECC-1	Protection System and Remedial Action Scheme Misoperation
PRC-005-1.1b	Transmission and Generation Protection System Maintenance and Testing
PRC-005-2(i)	Protection System Maintenance
PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance
PRC-006-2	Automatic Underfrequency Load Shedding
PRC-006-NPCC-1	Automatic Underfrequency Load Shedding
PRC-006-SERC-01	Automatic Underfrequency Load Shedding Requirements
PRC-008-0	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program
PRC-011-0	Undervoltage Load Shedding System Maintenance and Testing
PRC-015-0	Special Protection System Data and Documentation
PRC-016-0.1	Special Protection System Misoperations
PRC-017-0	Special Protection System Maintenance and Testing

PRC-018-1	Disturbance Monitoring Equipment Installation and Data Reporting
PRC-021-1	Under-Voltage Load Shedding Program Data
PRC-022-1	Under-Voltage Load Shedding Program Performance
PRC-023-3	Transmission Relay Loadability
PRC-025-1	Generator Relay Loadability
Transmission Operations (TOP)	
TOP-001-1a	Reliability Responsibilities and Authorities
TOP-002-2.1b	Normal Operations Planning
TOP-003-1	Planned Outage Coordination
TOP-004-2	Transmission Operations
TOP-005-2a	Operational Reliability Information
TOP-006-2	Monitoring System Conditions
TOP-007-0	Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations
TOP-007-WECC-1a	System Operating Limits
TOP-008-1	Response to Transmission Limit Violations
Transmission Planning (TPL)	
TPL-001-4	Transmission System Planning Performance Requirements
Voltage and Reactive (VAR)	
VAR-001-4.1	Voltage and Reactive Control
VAR-002-4	Generator Operation for Maintaining Network Voltage Schedules
VAR-002-WECC-2	Automatic Voltage Regulators (AVR)
VAR-501-WECC-2	Power System Stabilizer (PSS)

Exhibit C: Updated *Glossary of Terms Used in NERC Reliability Standards*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Glossary of Terms Used in NERC Reliability Standards

Updated May 17, 2016

Introduction:

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 May 17, 2016.

This reference is divided into two sections, and each section is organized in alphabetical order. The first section identifies all terms that have been adopted by the NERC Board of Trustees for use in continent-wide standards; the second section identifies all terms that have been adopted by the NERC Board of Trustees for use in regional standards. (WECC, NPCC and RF are the only Regions that have definitions approved by the NERC Board of Trustees. If other Regions develop definitions for approved Regional Standards using a NERC-approved standards development process, those definitions will be added to the Regional Definitions section of this glossary.)

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 approved" date added following a final Order approving the definition.

Immediately under each term is a link to the archive for the development of that term.

- Definitions that have been adopted by the NERC Board of Trustees but have not been approved by FERC, or FERC has not approved but has directed be modified, are shaded in blue.
- Definitions that have been remanded or retired are shaded in orange.
- Definitions that have been approved by FERC are white.

Any comments regarding this glossary should be reported to the following: sarcomm@nerc.com with "Glossary Comment" in the subject line.

Continent-wide Definitions:

Regional Definitions:

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Actual Frequency (F_A) [Archive]		2/11/2016		The Interconnection frequency measured in Hertz (Hz).
Actual Net Interchange (NI_A) [Archive]		2/11/2016		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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	A Balancing Authority Area that is interconnected another Balancing Authority Area either directly or via a multi-party agreement or transmission tariff.
Adjacent Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Adverse Reliability Impact [Archive]		8/4/2011		The impact of an event that results in Bulk Electric System instability or Cascading.
After the Fact [Archive]	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 [Archive]		2/8/2005	3/16/2007	A contract or arrangement, either written or verbal and sometimes enforceable by law.
Alternative Interpersonal Communication [Archive]		11/7/2012	4/16/2015 (Becomes effective 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 [Archive]		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 [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Area Control Error [Archive]	ACE	2/8/2005	3/16/2007 (Becomes inactive 3/31/14)	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.
Area Control Error [Archive]	ACE	12/19/2012	10/16/2013 (Becomes effective 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.
Area Interchange Methodology [Archive]		08/22/2008	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 [Archive]		5/2/2006	3/16/2007	The state where the Interchange Authority has received the Interchange information (initial or revised).
Arranged Interchange [Archive]		2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	The state where a Request for Interchange (initial or revised) has been submitted for approval.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Attaining Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 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 [Archive]	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 Generation Control [Archive]	AGC	2/11/2016		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.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Automatic Time Error Correction (I_{ATEC}) [Archive]		2/11/2016		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. $\mathbf{I}_{ATEC} = \frac{\mathbf{PII}_{accum}^{on/off\ peak}}{(1-Y)*H}$ when operating in Automatic Time Error Correction Mode. The absolute value of $\mathbf{I}_{ATEC}$ shall not exceed L_{max} . $\mathbf{I}_{ATEC}$ shall be zero when operating in any other AGC mode. • L_{max} is the maximum value allowed for $\mathbf{I}_{ATEC}$ set by each BA between $0.2*\lvert B_i\rvert$ and L_{10}, $0.2*\lvert B_i\rvert \leq L_{max} \leq L_{10}$. • $L_{10} = 1.65* \varepsilon_{10}\sqrt{(-10B_i)(-10B_S)}$. • $\varepsilon 10$ is a constant derived from the targeted frequency bound. It is the targeted root-mean-square (RMS) value of ten-minute average frequency error based on frequency performance over a given year. The bound, ε 10, is the same for every Balancing Authority Area within an Interconnection. • $Y = B_i / B_S$. • H = Number of hours used to payback primary inadvertent interchange energy. The value of H is set to 3. (*Continued below*)

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Automatic Time Error Correction (I_{ATEC}) *Continued…* [Archive]		2/11/2016		• B_i = Frequency Bias Setting for the Balancing Authority Area (MW / 0.1 Hz). • B_S = Sum of the minimum Frequency Bias Settings for the Interconnection (MW / 0.1 Hz). • Primary Inadvertent Interchange (PII_{hourly}) is (1-Y) * (II_{actual} - B_i * ΔTE/6) • II_{actual} is the hourly Inadvertent Interchange for the last hour. ΔTE is the hourly change in system Time Error as distributed by the Interconnection time monitor,where: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t)*(TE_{offset})$ • TD_{adj} is the Reliability Coordinator adjustment for differences with Interconnection time monitor control center clocks. • t is the number of minutes of manual Time Error Correction that occurred during the hour. • TE_{offset} is 0.000 or +0.020 or -0.020. • PII_{accum} is the Balancing Authority Area's accumulated PII_{hourly} in MWh. An On-Peak and Off-Peak accumulation accounting is required, where: $\mathbf{PII}_{accum}^{on/offpeak} = last\ period's\ \mathbf{PII}_{accum}^{on/offpeak} + \mathbf{PII}_{hourly}$

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
Available Flowgate Capability [Archive]	AFC	08/22/2008	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 [Archive]	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.
Available Transfer Capability [Archive]	ATC	08/22/2008	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 [Archive]	ATCID	08/22/2008	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.

Continent-wide Term	Acronym	BOT Approval Date	FERC Approval Date	Definition
ATC Path [Archive]		08/22/2008	Not approved; Modification directed 11/24/09	Any combination of Point of Receipt and Point of Delivery for which ATC is calculated; and any Posted Path[1].

[1] See 18 CFR 37.6(b)(1)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Balancing Authority [Archive]	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 [Archive]		2/11/2016		The responsible entity that integrates resource plans ahead of time, maintains Demand and resource balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
Balancing Authority Area [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Balancing Contingency Event [Archive]		11/5/2015		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 [Archive]		2/8/2005	3/16/2007	The minimum amount of electric power delivered or required over a given period at a constant rate.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
BES Cyber Asset [Archive]		11/26/2012	11/22/2013 (Becomes effective 4/1/2016)	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. (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.)
BES Cyber Asset [Archive]	BCA	2/12/2015	1/21/2016 (effective 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 [Archive]		11/26/2012	11/22/2013 (Becomes effective 4/1/2016)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
BES Cyber System Information [Archive]		11/26/2012	11/22/2013 (Becomes effective 4/1/2016)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
Blackstart Capability Plan [Archive]		2/8/2005 Will be retired when EOP-005-2 becomes enforceable on (7/1/13)	3/16/2007	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Blackstart Resource [Archive]		8/5/2009	3/17/2011	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.
Blackstart Resource [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		08/22/2008	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).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System [Archive]	BES	2/8/2005	3/16/2007 (Becomes inactive on 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System[2] [Archive]	BES	01/18/2012	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.

[2] 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			**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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			• **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:

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System [Archive]	BES	11/21/2013	3/20/14 (Becomes effective 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. • **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:

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			a) The individual resources, and b) The system designed primarily for delivering capacity from the point where those resources aggregate to greater than 75 MVA to a common point of connection at a voltage of 100 kV or above. • **I5** –Static or dynamic devices (excluding generators) dedicated to supplying or absorbing Reactive Power that are connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, or through a transformer that is designated in Inclusion I1 unless excluded by application of Exclusion E4. **Exclusions:** • **E1** - Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and: a) Only serves Load. Or, b) Only includes generation resources, not identified in Inclusions I2, I3, or I4, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or, c) Where the radial system serves Load and includes generation resources, not identified in Inclusions I2, I3 or I4, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			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. • **E2** - A generating unit or multiple generating units on the customer's side of the retail meter that serve all or part of the retail Load with electric energy if: (i) the net capacity provided to the BES does not exceed 75 MVA, and (ii) standby, back-up, and maintenance power services are provided to the generating unit or multiple generating units or to the retail Load by a Balancing Authority, or provided pursuant to a binding obligation with a Generator Owner or Generator Operator, or under terms approved by the applicable regulatory authority. • **E3** - Local networks (LN): A group of contiguous transmission Elements operated at less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN's emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customers and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following: a) Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusions I2, I3, or I4 and do not have an aggregate capacity of non-retail

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk Electric System **(Continued)**	BES			generation greater than 75 MVA (gross nameplate rating); b) Real Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and c) Not part of a Flowgate or transfer path: The LN does not contain any part of a permanent Flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection, or a comparable monitored Facility in the ERCOT or Quebec 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 [Archive]		5/9/2013	7/9/2013	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Bulk-Power System [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		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.
Business Practices [Archive]		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.
Bus-tie Breaker [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/2015)	A circuit breaker that is positioned to connect two individual substation bus configurations.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Capacity Benefit Margin [Archive]	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 [Archive]	CBMID	11/13/2008	11/24/2009	A document that describes the implementation of a Capacity Benefit Margin methodology.
Capacity Emergency [Archive]		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 [Archive]		2/8/2005	3/16/2007	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Cascading [Archive]		11/5/2015	1/21/2016 (effective 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.
Cascading Outages [Archive]		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.~~
CIP Exceptional Circumstance [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Compliance Monitor [Archive]		2/8/2005	3/16/2007	The entity that monitors, reviews, and ensures compliance of responsible entities with reliability standards.
Composite Confirmed Interchange [Archive]		2/6/2014	6/30/2014 (Becomes effective 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 [Archive]		8/14/2014	5/13/2015 (Becomes effective 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 [Archive]		5/2/2006	3/16/2007	The state where the Interchange Authority has verified the Arranged Interchange.
Confirmed Interchange [Archive]		2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	The state where no party has denied and all required parties have approved the Arranged Interchange.
Congestion Management Report [Archive]		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 [Archive]		8/4/2011	10/17/2013 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Constrained Facility [Archive]		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 [Archive]		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 [Archive]		11/5/2015		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 [Archive]		2/8/2005	3/16/2007	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Contingency Reserve [Archive]				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 [Archive]		11/5/2015		A period not exceeding 90 minutes following the end of the Contingency Event Recovery Period.
Contract Path [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Control Center [Archive]		11/26/12	11/22/13 (Becomes effective 4/1/16)	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 [Archive]	CPS	2/8/2005	3/16/2007	The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period.
Corrective Action Plan [Archive]		2/7/2006	3/16/2007	A list of actions and an associated timetable for implementation to remedy a specific problem.
Cranking Path [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.
Critical Assets [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	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 [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	Cyber Assets essential to the reliable operation of Critical Assets.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Curtailment [Archive]		2/8/2005	3/16/2007	A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.
Curtailment Threshold [Archive]		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 [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Assets [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	Programmable electronic devices, including the hardware, software, and data in those devices.
Cyber Security Incident [Archive]		5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Cyber Security Incident [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Delayed Fault Clearing [Archive]		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 [Archive]		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 [Archive]	DSM	2/8/2005	3/16/2007	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.
Demand-Side Management [Archive]	DSM	5/6/2014	2/19/2015 (Becomes effective 7/1/16)	All activities or programs undertaken by any applicable entity to achieve a reduction in Demand.
Dial-up Connectivity [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Dispatch Order [Archive]		08/22/2008	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 [Archive]		2/8/2005	3/16/2007	Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.
Distribution Factor [Archive]	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 [Archive]	DP	2/8/2005	3/16/2007	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.
Distribution Provider [Archive]	DP	11/5/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Disturbance [Archive]		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 [Archive]	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 [Archive]	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[3]: • 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

[3] Phasor Measurement Units and any other equipment that meets the functional requirements of DMEs may qualify as DMEs.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Dynamic Interchange Schedule or Dynamic Schedule [Archive]		2/8/2005	3/16/2007	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.
Dynamic Interchange Schedule or Dynamic Schedule [Archive]		2/6/2014	6/30/2014 (Becomes effective 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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Economic Dispatch [Archive]		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 [Archive]	EACMS	11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]	EAP	11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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.
Electrical Energy [Archive]		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 [Archive]	ESP	5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Electronic Security Perimeter [Archive]	ESP	11/26/12	11/22/2013 (Becomes effective 4/1/2016)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Element [Archive]		2/8/2005	3/16/2007	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.
Element [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		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 [Archive]		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 [Archive]	Emergency RFI	10/29/2008	12/17/2009	Request for Interchange to be initiated for Emergency or Energy Emergency conditions.
Energy Emergency [Archive]		2/8/2005	3/16/2007	A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements.
Energy Emergency [Archive]		11/13/2014	11/19/2015 effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Equipment Rating [Archive]		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 [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]	ETC	08/22/2008	11/24/2009	Committed uses of a Transmission Service Provider's Transmission system considered when determining ATC or AFC.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Facility [Archive]		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 [Archive]		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 [Archive]		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 [Archive]		2/7/2006	3/16/2007	The likelihood that a fire will ignite or spread in a particular geographic area.
Firm Demand [Archive]		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 [Archive]		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 [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Flowgate [Archive]		08/22/2008	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 [Archive]		08/22/2008	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 [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Bias Setting [Archive]		2/8/2005	3/16/2007 (Becomes inactive 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.
Frequency Bias Setting [Archive]		2/7/2013	1/16/2014 (Becomes effective 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 [Archive]		2/8/2005	3/16/2007	A change in Interconnection frequency.
Frequency Error [Archive]		2/8/2005	3/16/2007	The difference between the actual and scheduled frequency. ($F_A - F_S$)
Frequency Regulation [Archive]		2/8/2005	3/16/2007	The ability of a Balancing Authority to help the Interconnection maintain Scheduled Frequency. This assistance can include both turbine governor response and Automatic Generation Control.
Frequency Response [Archive]		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).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Response Measure [Archive]	FRM	2/7/2013	1/16/2014 (Becomes effective 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 [Archive]	FRO	2/7/2013	1/16/2014 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Response Sharing Group [Archive]	FRSG	2/7/2013	1/16/2014 (Becomes effective 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 [Archive]	GOP	2/8/2005	3/16/2007	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
Generator Operator [Archive]	GOP	11/5/2015	1/21/2016 (effective 7/1/2016)	The entity that operates generating Facility(ies) and performs the functions of supplying energy and Interconnected Operations Services.
Generator Owner [Archive]	GO	2/8/2005	3/16/2007	Entity that owns and maintains generating units.
Generator Owner [Archive]	GO	11/5/2015	1/21/2016 (effective 7/1/2016)	Entity that owns and maintains generating Facility(ies).
Generator Shift Factor [Archive]	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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Generation Capability Import Requirement [Archive]	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.
Host Balancing Authority [Archive]		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 [Archive]		2/8/2005	3/16/2007	Data measured on a Clock Hour basis.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Implemented Interchange [Archive]		5/2/2006	3/16/2007	The state where the Balancing Authority enters the Confirmed Interchange into its Area Control Error equation.
Inadvertent Interchange [Archive]		2/8/2005	3/16/2007	The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. ($I_A - I_S$)
Independent Power Producer [Archive]	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. [Archive]	IEEE	2/7/2006	3/16/2007	

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interactive Remote Access [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]		5/2/2006	3/16/2007	Energy transfers that cross Balancing Authority boundaries.
Interchange Authority [Archive]	IA	5/2/2006	3/16/2007	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.
Interchange Authority [Archive]	IA	11/5/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interchange Distribution Calculator [Archive]	IDC	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}) [Archive]		2/11/2016		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 [Archive]		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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	The details of an Interchange Transaction required for its physical implementation.
Interconnected Operations Service [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interconnected Operations Service [Archive]		11/5/2015	1/21/2016 (effective 7/1/2016)	A service (exclusive of basic energy and Transmission Services) that is required to support the Reliable Operation of interconnected Bulk Electric Systems.
Interconnection [Archive]		2/8/2005	3/16/2007 (Retires 6/30/2016)	When capitalized, any one of the three major electric system networks in North America: Eastern, Western, and ERCOT.
Interconnection [Archive]		8/15/2013	4/16/2015 (Effective 7/1/2016)	When capitalized, any one of the four major electric system networks in North America: Eastern, Western, ERCOT and Quebec.
Interconnection [Archive]		11/5/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interconnection Reliability Operating Limit [Archive]	IROL	2/8/2005	3/16/2007 Retired 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.
Interconnection Reliability Operating Limit [Archive]	IROL	11/1/2006	12/27/2007	A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages[4] that adversely impact the reliability of the Bulk Electric System.
Interconnection Reliability Operating Limit T_V [Archive]	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 [Archive]		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.
Intermediate Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	A Balancing Authority on the scheduling path of an Interchange Transaction other than the Source Balancing Authority and Sink Balancing Authority.

[4] On September 13, 2012, FERC issued an Order approving NERC's request to modify the reference to "Cascading Outages" to "Cascading outages" within the definition of IROL due to the fact that the definition of "Cascading Outages" was previously remanded by FERC.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Intermediate System [Archive]		11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]		11/7/2012	4/16/2015 (Becomes effective 10/1/2015)	Any medium that allows two or more individuals to interact, consult, or exchange information.
Interruptible Load or Interruptible Demand [Archive]		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 [Archive]		2/8/2005	3/16/2007	Automatic Generation Control of jointly owned units by two or more Balancing Authorities.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Limiting Element [Archive]		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 [Archive]		2/8/2005	3/16/2007	An end-use device or customer that receives power from the electric system.
Load Shift Factor [Archive]	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 [Archive]	LSE	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.
Load-Serving Entity [Archive]	LSE	11/5/2015	1/21/2016 (effective 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 [Archive]		8/4/2011	10/17/2013 (Becomes effective 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.
Low Impact BES Cyber System Electronic Access Point [Archive]	LEAP	2/12/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Low Impact External Routable Connectivity [Archive]	LERC	2/12/2015	1/21/2016 (effective 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 [Archive]		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 [Archive]	MVCD	11/3/2011	3/21/2013 (Becomes effective 7/1/14)	The calculated minimum distance stated in feet (meters) to prevent flash-over between conductors and vegetation, for various altitudes and operating voltages.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Misoperation [Archive]		2/7/2006	3/16/2007	• 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Misoperation [Archive]		8/14/2014	5/13/2015 (Becomes effective 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***)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Continued… Misoperation [Archive]		8/14/2014	5/13/2015 (Becomes effective 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.
Most Severe Single Contingency [Archive]	MSSC	11/5/2015		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).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Native Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Native Load [Archive]		2/8/2005	3/16/2007	The end-use customers that the Load-Serving Entity is obligated to serve.
Near-Term Transmission Planning Horizon [Archive]		1/24/2011	11/17/2011	The transmission planning period that covers Year One through five.
Net Actual Interchange [Archive]		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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.
Net Scheduled Interchange [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Non-Consequential Load Loss [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	1. That generating reserve not connected to the system but capable of serving demand within a specified time. 2. Interruptible load that can be removed from the system in a specified time.
Normal Clearing [Archive]		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 [Archive]		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 [Archive]		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) [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Nuclear Plant Licensing Requirements [Archive]	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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Off-Peak [Archive]		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 [Archive]		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 [Archive]	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 [Archive]	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 [Archive]		5/6/2014	4/16/2015 (Becomes effective 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.)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Operating Plan [Archive]		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 [Archive]		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 [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Operating Reserve – Spinning [Archive]		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 [Archive]		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 [Archive]		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 [Archive]		10/17/2008	3/17/2011	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.).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Operational Planning Analysis [Archive]		2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	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, Interchange, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.).
Operational Planning Analysis [Archive]		11/13/2014	11/19/2015 (Becomes effective 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 [Archive]		2/6/2014	6/19/2014 (effective 7/1/2016)	Individuals who perform current day or next day outage coordination or assessments, or who determine SOLs, IROLs, or operating nomograms,[1] in direct support of Real-time operations of the Bulk Electric System.
Outage Transfer Distribution Factor [Archive]	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).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Overlap Regulation Service [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Participation Factors [Archive]		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 [Archive]		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 [Archive]		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 [Archive]	PACS	11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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 [Archive]	PSP	5/2/2006	1/18/2008 (Becomes inactive 3/31/2016)	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.
Physical Security Perimeter [Archive]	PSP	11/26/12	11/22/2013 (Becomes effective 4/1/2016)	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Planning Assessment [Archive]		8/4/2011	10/17/2013 (Becomes effective 1/1/15)	Documented evaluation of future Transmission System performance and Corrective Action Plans to remedy identified deficiencies.
Planning Authority [Archive]	PA	2/8/2005	3/16/2007	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
Planning Authority [Archive]	PA	11/5/2015	1/21/2016 (effective 7/1/2016)	The responsible entity that coordinates and integrates transmission Facilities and service plans, resource plans, and Protection Systems.
Planning Coordinator [Archive]	PC	8/22/2008	11/24/2009	See Planning Authority.
Point of Delivery [Archive]	POD	2/8/2005	3/16/2007	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.
Point of Receipt [Archive]	POR	2/8/2005	3/16/2007	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.
Point of Receipt [Archive]	POR	11/5/2015	1/21/2016 (effective 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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Postback [Archive]		08/22/2008	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.
Power Transfer Distribution Factor [Archive]	PTDF	08/22/2008	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 [Archive]		11/5/2015		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protected Cyber Assets [Archive]	PCA	11/26/2012	11/22/2013 (Becomes effective 4/1/16)	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.
Protected Cyber Assets [Archive]	PCA	2/12/2015	1/21/2016 (effective 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 [Archive]		2/7/2006	3/17/2007 retired 4/1/2013	Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System [Archive] [Implementation Plan]		11/19/2010	2/3/2012 (Became effective on 4/1/13)	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 Coordination Study [Archive]		11/5/2015		An analysis to determine whether Protection Systems operate in the intended sequence during Faults.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program (PRC-005-2) [Archive]	PSMP	11/7/2012	12/19/2013 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program (PRC-005-3) [Archive]	PSMP	11/7/2013	1/22/2015 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program (PRC-005-4) [Archive]	PSMP	11/13/2014	9/17/2015 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Protection System Maintenance Program (PRC-005-6) [Archive]	PSMP	11/5/2015	12/18/2015 (Becomes effective 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 [Archive]		2/8/2005	3/16/2007	A telemetered reading or value that is updated in real time and used as a "virtual" tie line flow in the AGC/ACE equation but for which no physical tie or energy metering actually exists. The integrated value is used as a metered MWh value for interchange accounting purposes.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Pseudo-Tie [Archive]		2/6/2014	6/30/2014 (Becomes effective 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).
Pseudo-Tie [Archive]		2/11/2016		A time-varying energy transfer that is updated in Real-time and included in the Actual Net Interchange term (NIA) in the same manner as a Tie Line in the affected Balancing Authorities' Reporting ACE equation (or alternate control processes).
Purchasing-Selling Entity [Archive]	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 [Archive]		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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	The operational limits of a transmission system element under a set of specified conditions.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Rated System Path Methodology [Archive]		08/22/2008	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 [Archive]		2/8/2005	3/16/2007	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).
Reactive Power [Archive]		11/5/2015	1/21/2016 (effective 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).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Real Power [Archive]		2/8/2005	3/16/2007	The portion of electricity that supplies energy to the load.
Real Power [Archive]		11/5/2015	1/21/2016 (effective 7/1/2016)	The portion of electricity that supplies energy to the Load.
Reallocation [Archive]		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 [Archive]		2/7/2006	3/16/2007	Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)
Real-time Assessment [Archive]		10/17/2008	3/17/2011	An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data
Real-time Assessment [Archive]		11/13/2014	Revised definition. 11/19/2015 (Becomes effective 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.)
Receiving Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority importing the Interchange.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Regional Reliability Organization [Archive]	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 [Archive]		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 [Archive]		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 [Archive]		8/15/2013	4/16/2015 (Becomes effective 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 [Archive]		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 [Archive]		2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	A request to modify a Confirmed Interchange or Implemented Interchange for reliability purposes.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reliability Adjustment RFI [Archive]		10/29/2008	12/17/2009	Request to modify an Implemented Interchange Schedule for reliability purposes.
Reliability Coordinator [Archive]	RC	2/8/2005	3/16/2007	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 Coordinator [Archive]	RC	11/5/2015	1/21/2016 (effective 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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reliability Coordinator Information System [Archive]	RCIS	2/8/2005	3/16/2007	The system that Reliability Coordinators use to post messages and share operating information in real time.
Reliability Directive [Archive]		8/16/2012	11/19/2015 (Becomes inactive 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 [Archive]		5/9/2013	7/9/2013	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reliability Standard [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		5/9/2013	7/9/2013	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.
Reliable Operation [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]	RAS	2/8/2005	3/16/2007	See “Special Protection System”

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Remedial Action Scheme [Archive]	RAS	11/13/2014	11/19/2015 effective 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

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Continued Remedial Action Scheme [Archive]				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)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Continued Remedial Action Scheme [Archive]				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 [Archive]		2/12/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reportable Balancing Contingency Event [Archive]		11/5/2015		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
Reportable Cyber Security Incident [Archive]		11/26/2012	11/22/2013 (Becomes effective 4/1/16)	A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.
Reportable Disturbance [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE [Archive]		8/15/2013	4/16/2015 (Becomes effective 7/1/2016)	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: $\text{Reporting ACE} = (NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME}$ Reporting ACE is calculated in the Western Interconnection as follows: $\text{Reporting ACE} = (NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME} + I_{ATEC}$ 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

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE **(Continued)**				Interchange Actual. **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. $I_{ATEC} = \frac{PII_{accum}^{on/off\ peak}}{(1-Y)*H}$ when operating in Automatic Time Error Correction control mode. **I_{ATEC}** shall be zero when operating in any other AGC mode. • Y = B / BS. • H = Number of hours used to payback Primary Inadvertent Interchange energy. The value of H is set to 3. • BS = Frequency Bias for the Interconnection (MW / 0.1 Hz).

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE **(Continued)**				• 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: $\Delta TE = TE_{end\ hour} - TE_{begin\ hour} - TD_{adj} - (t)*(TE_{offset})$ • TD_{adj} is the Reliability Coordinator adjustment for differences with Interconnection Time Monitor control center clocks. • t is the number of minutes of Manual Time Error Correction that occurred during the hour. • TE_{offset} is 0.000 or +0.020 or -0.020. • PII_{accum} is the Balancing Authority's accumulated PII_{hourly} in MWh. An On-Peak and Off-Peak accumulation accounting is required. Where: $PII_{accum}^{on/off\ peak} = \text{last period's } PII_{accum}^{on/off peak} + PII_{hourly}$ All NERC Interconnections with multiple Balancing Authorities operate using the principles of Tie-line Bias (TLB) Control and require the use of an ACE equation similar to the Reporting ACE defined above. Any modification(s) to this specified Reporting ACE equation that is(are) implemented for all BAs on an Interconnection and is(are) consistent with the following four principles will provide a valid alternative Reporting ACE equation

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE **(Continued)**				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.)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reporting ACE [Archive]		2/11/2016		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 = $(NI_A - NI_S) - 10B(F_A - F_S) - I_{ME}$ 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. • 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
				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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Request for Interchange [Archive]	RFI	2/6/2014	6/30/2014 (Becomes effective 10/1/2014)	A collection of data as defined in the NAESB Business Practice Standards submitted for the purpose of implementing bilateral Interchange between Balancing Authorities or an energy transfer within a single Balancing Authority.
Reserve Sharing Group [Archive]	RSG	2/8/2005	3/16/2007	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 [Archive]		11/5/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Reserve Sharing Group Reporting ACE [Archive]		8/15/2013	4/16/2015 (Becomes effective 7/1/2016)	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.
Reserve Sharing Group Reporting ACE [Archive]		11/5/2015	1/21/2016 (effective 7/1/2016)	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 [Archive]	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.
Resource Planner [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		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 [Archive]	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Right-of-Way [Archive]	ROW	11/3/2011	3/21/2013 (Becomes inactive 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.
Right-of-Way [Archive]	ROW	5/9/12	3/21/2013 (Becomes effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Scenario [Archive]		2/7/2006	3/16/2007	Possible event.
Schedule [Archive]		2/8/2005	3/16/2007	(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.
Scheduled Frequency [Archive]		2/8/2005	3/16/2007	60.0 Hertz, except during a time correction.
Scheduled Net Interchange (NI_S) [Archive]		2/11/2016		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 [Archive]		2/8/2005	3/16/2007	An entity responsible for approving and implementing Interchange Schedules.
Scheduling Path [Archive]		2/8/2005	3/16/2007	The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.
Sending Balancing Authority [Archive]		2/8/2005	3/16/2007	The Balancing Authority exporting the Interchange.
Sink Balancing Authority [Archive]		2/8/2005	3/16/2007	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.)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Sink Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 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 [Archive]		2/8/2005	3/16/2007	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.)
Source Balancing Authority [Archive]		2/6/2014	6/30/2014 (Becomes effective 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) [Archive]	SPS	2/8/2005	3/16/2007	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Special Protection System (Remedial Action Scheme) [Archive]	SPS	5/5/2016		See "Remedial Action Scheme"
Spinning Reserve [Archive]		2/8/2005	3/16/2007	Unloaded generation that is synchronized and ready to serve additional demand.
Stability [Archive]		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 [Archive]		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 [Archive]	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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Sustained Outage [Archive]		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 [Archive]		2/8/2005	3/16/2007	A combination of generation, transmission, and distribution components.
System Operating Limit [Archive]	SOL	2/8/2005	3/16/2007	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)

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
System Operating Limit [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		2/8/2005	3/16/2007	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
System Operator [Archive]		2/6/2014	6/19/2014 (effective 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 [Archive]		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 [Archive]		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 [Archive]		2/8/2005	3/16/2007	A circuit connecting two Balancing Authority Areas.
Tie Line Bias [Archive]		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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Time Error Correction [Archive]		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)[5] Log [Archive]		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 [Archive]	TFC	08/22/2008	11/24/2009	The maximum flow capability on a Flowgate, is not to exceed its thermal rating, or in the case of a flowgate used to represent a specific operating constraint (such as a voltage or stability limit), is not to exceed the associated System Operating Limit.
Total Internal Demand [Archive]		5/6/2014	2/19/2015 (Becomes effective 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 [Archive]	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 [Archive]		2/8/2005	3/16/2007	See Interchange Transaction.

[5] NERC added the spelled out term for TLR Log for clarification purposes.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transfer Capability [Archive]		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 [Archive]		2/8/2005	3/16/2007	See Distribution Factor.
Transient Cyber Asset [Archive]		2/12/2015	1/21/2016 (effective 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 [Archive]		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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transmission Constraint [Archive]		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 [Archive]		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 Customer [Archive]		11/5/2015	1/21/2016 (effective 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 [Archive]		2/7/2006	3/16/2007	A system of structures, wires, insulators and associated hardware that carry electric energy from one point to another in an electric power system. Lines are operated at relatively high voltages varying from 69 kV up to 765 kV, and are capable of transmitting large quantities of electricity over long distances.
Transmission Operator [Archive]	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 Operator [Archive]	TOP	11/5/2015	1/21/2016 (effective 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transmission Operator Area [Archive]		08/22/2008	11/24/2009	The collection of Transmission assets over which the Transmission Operator is responsible for operating.
Transmission Owner [Archive]	TO	2/8/2005	3/16/2007	The entity that owns and maintains transmission facilities.
Transmission Owner [Archive]	TO	11/5/2015	1/21/2016 (effective 7/1/2016)	The entity that owns and maintains transmission Facilities.
Transmission Planner [Archive]	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 Planner [Archive]	TP	11/5/2015	1/21/2016 (effective 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 [Archive]	TRM	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 [Archive]	TRMID	08/22/2008	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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Transmission Service [Archive]		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 [Archive]	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.
Transmission Service Provider [Archive]	TSP	11/5/2015	1/21/2016 (effective 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 [Archive]	UVLS Program	11/13/2014	11/19/2015 effective 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 [Archive]		2/7/2006	3/16/2007	All plant material, growing or not, living or dead.
Vegetation Inspection [Archive]		2/7/2006	3/16/2007	The systematic examination of a transmission corridor to document vegetation conditions.
Vegetation Inspection [Archive]		11/3/2011	3/21/2013 (Becomes inactive 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.

Continent-wide Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Vegetation Inspection [Archive]		5/9/12	3/21/2013 (Becomes effective 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 [Archive]		2/8/2005	3/16/2007	The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits.
Year One [Archive]		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.

ERCOT Regional Definitions

The following terms were developed as regional definitions for the ERCOT region:

ERCOT Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Frequency Measurable Event [Archive]	FME	8/15/2013	1/16/2014 (Becomes effective 4/1/14)	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 [Archive]		8/15/2013	1/16/2014 (Becomes effective	The electronic, digital or mechanical device that implements Primary Frequency Response of generating units/generating facilities or other system elements.

ERCOT Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
			4/1/14)	
Primary Frequency Response [Archive]	PFR	8/15/2013	1/16/2014 (Becomes effective 4/1/14)	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.

NPCC Regional Definitions

The following definitions were developed for use in NPCC Regional Standards.

NPCC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Current Zero Time [Archive]		11/04/2010	10/20/2011	The time of the final current zero on the last phase to interrupt.
Generating Plant [Archive]		11/04/2010	10/20/2011	One or more generators at a single physical location whereby any single contingency can affect all the generators at that location.

Reliability*First* Regional Definitions

The following definitions were developed for use in Reliability*First* Regional Standards.

RFC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Resource Adequacy [Archive]		08/05/2009	03/17/2011	The ability of supply-side and demand-side resources to meet the aggregate electrical demand (including losses)
Net Internal Demand [Archive]		08/05/2009	03/17/2011	Total of all end-use customer demand and electric system losses within specified metered boundaries, less Direct Control Management and Interruptible Demand
Peak Period [Archive]		08/05/2009	03/17/2011	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 [Archive]		11/03/2011		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 [Archive]		08/05/2009	03/17/2011	The planning year that begins with the upcoming annual Peak Period

WECC Regional Definitions

The following definitions were developed for use in WECC Regional Standards.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Area Control Error† [Archive]	ACE	3/12/2007	6/8/2007 (Becomes inactive 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‡ [Archive]	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 [Archive]		3/26/2008	5/21/2009 (Becomes inactive 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 [Archive]		12/19/2012	10/16/2013 (Becomes effective 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‡ [Archive]		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‡ [Archive]		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.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Commercial Operation [Archive]		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 [Archive]		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 [Archive]		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† [Archive]		3/12/2007	6/8/2007	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.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Extraordinary Contingency‡ [Archive]		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).*
Frequency Bias‡ [Archive]		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 [Archive]	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 [Archive]	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

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
				mitigation to comply with all Reliability Standards. • Each RAS may have different components and operating characteristics.
Generating Unit Capability‡ [Archive]		3/12/2007	6/8/2007	Means the MVA nameplate rating of a generator.
Non-spinning Reserve‡ [Archive]		3/12/2007	6/8/2007	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‡ [Archive]		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‡ [Archive]		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‡ [Archive]	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.

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Primary Inadvertent Interchange [Archive]		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 [Archive]		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 [Archive]		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 [Archive]		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.
Relief Requirement [Archive]		2/10/2009	3/17/2011 (Becomes inactive 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 [Archive]		2/7/2013	6/13/2014 (Becomes effective 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		3/26/2008	5/21/2009	The component of area (n) inadvertent interchange caused by

WECC Regional Term	Acronym	BOT Approved Date	FERC Approved Date	Definition
Interchange [Archive]				the regulating deficiencies of area (i).
Security-Based Misoperation [Archive]		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[†] [Archive]		3/12/2007	6/8/2007	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 [Archive]	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[†] [Archive]		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

Version	Date	Action
1.2	May 5, 2016	**Board Adopted:** Special Protection System (SPS)
1.1	April 1, 2016	**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
1.0	March 31, 2016	**Inactive**: Critical Assets, Critical Cyber Assets, Cyber Assets, Cyber Security Incident, Electronic Security Perimeter, Physical Security Perimeter