

**A. Introduction**

1. **Title:** Automatic Generation Control
2. **Number:** BAL-005-0.2b
3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.
4. **Applicability:**
  - 4.1. Balancing Authorities
  - 4.2. Generator Operators
  - 4.3. Transmission Operators
  - 4.4. Load Serving Entities
5. **Effective Date:** May 13, 2009

**B. Requirements**

- R1.** All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.
  - R1.1.** Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.
  - R1.2.** Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.
  - R1.3.** Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.
- R2.** Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retired)
- R3.** A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.
- R4.** A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.
- R5.** A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.
- R6.** The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

- R7.** The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.
- R8.** The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.
- R8.1.** Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.
- R9.** The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
- R9.1.** Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.
- R10.** The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.
- R11.** Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.
- R12.** Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
- R12.1.** Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.
- R12.2.** Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.
- R12.3.** Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.
- R13.** Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error ( $I_{ME}$ ) term of the ACE equation to compensate for any equipment error until repairs can be made.
- R14.** The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.
- R15.** The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

- R16.** The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.
- R17.** Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	$\leq 0.001$ Hz
MW, MVAR, and voltage transducer	$\leq 0.25$ % of full scale
Remote terminal unit	$\leq 0.25$ % of full scale
Potential transformer	$\leq 0.30$ % of full scale
Current transformer	$\leq 0.50$ % of full scale

**C. Measures**

Not specified.

**D. Compliance**

**1. Compliance Monitoring Process**

**1.1. Compliance Monitoring Responsibility**

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

- 1.1.1.** Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.
- 1.1.2.** Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

**1.2. Compliance Monitoring Period and Reset Timeframe**

Not specified.

**1.3. Data Retention**

- 1.3.1.** Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.
- 1.3.2.** Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

## Standard BAL-005-0.2b — Automatic Generation Control

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

### 1.4. Additional Compliance Information

Not specified.

### 2. Levels of Non-Compliance

Not specified.

## E. Regional Differences

None identified.

## F. Associated Documents

- Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

### Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added “1.”; changed hyphen to “en dash.” Changed font style for “Appendix 1” to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to “0.1b”	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from “BAL-005-1” to “BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## Appendix 1

Effective Date: August 27, 2008 (U.S.)

### Interpretation of BAL-005-0 Automatic Generation Control, R17

#### Request for Clarification received from PGE on July 31, 2007

*PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:*

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

#### **BAL-005-0**

**R17.** Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

<b>Device</b>	<b>Accuracy</b>
Digital frequency transducer	$\leq 0.001$ Hz
MW, MVAR, and voltage transducer	$\leq 0.25\%$ of full scale
Remote terminal unit	$\leq 0.25\%$ of full scale
Potential transformer	$\leq 0.30\%$ of full scale
Current transformer	$\leq 0.50\%$ of full scale

#### **Existing Interpretation Approved by Board of Trustees May 2, 2007**

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to “annually check and calibrate” does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to “annually check and calibrate” the devices listed in the table, unless they are included in the control center time error and frequency devices.

#### **Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007**

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system

## **Standard BAL-005-0.2b — Automatic Generation Control**

---

operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

## A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-3
3. **Purpose:** Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability:**
  - 4.1. Within the text of Standard CIP-003-3, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity.
  - 4.2. The following are exempt from Standard CIP-003-3:
    - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
  - R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

- R1.2.** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)
  - R1.3.** Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
- R2.** Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.
  - R2.1.** The senior manager shall be identified by name, title, and date of designation.
  - R2.2.** Changes to the senior manager must be documented within thirty calendar days of the effective date.
  - R2.3.** Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
  - R2.4.** The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.
- R3.** Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)
  - R3.1.** Exceptions to the Responsible Entity’s cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)
  - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)
  - R3.3.** Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)
- R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
  - R4.1.** The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
  - R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)
  - R4.3.** The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
- R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
  - R5.1.** The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

- R5.1.1.** Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.
  - R5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
- R5.2.** The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
- R5.3.** The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
- R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

### C. Measures

- M1.** The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)
- M2.** The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)
- M4.** The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.
- M5.** The Responsible Entity shall make available its access control documentation as specified in Requirement R5.
- M6.** The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

### D. Compliance

#### 1. Compliance Monitoring Process

##### 1.1. Compliance Enforcement Authority

- 1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2** ERO for Regional Entity.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

##### 1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

##### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

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

**1.4. Data Retention**

- 1.4.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

- 1.5.1** None

**2. Violation Severity Levels (To be developed later.)**

**E. Regional Variances**

None identified.

**Version History**

Version	Date	Action	Change Tracking
2		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. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

3	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	
---	-----	--	--

## A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-4
3. **Purpose:** Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability:**
  - 4.1. Within the text of Standard CIP-003-4, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity.
  - 4.2. The following are exempt from Standard CIP-003-4:
    - 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 In nuclear plants, 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
    - 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

- R1.1.** The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
- R1.2.** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)
- R1.3.** Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
- R2.** Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
  - R2.1.** The senior manager shall be identified by name, title, and date of designation.
  - R2.2.** Changes to the senior manager must be documented within thirty calendar days of the effective date.
  - R2.3.** Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
  - R2.4.** The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.
- R3.** Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)
  - R3.1.** Exceptions to the Responsible Entity’s cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)
  - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)
  - R3.3.** Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)
- R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
  - R4.1.** The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
  - R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)
  - R4.3.** The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
- R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

- R5.1.** The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
  - R5.1.1.** Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.
  - R5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
- R5.2.** The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
- R5.3.** The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
- R6.** Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

### C. Measures

- M1.** The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)
- M2.** The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)
- M4.** The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.
- M5.** The Responsible Entity shall make available its access control documentation as specified in Requirement R5.
- M6.** The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

## **D. Compliance**

### **1. Compliance Monitoring Process**

#### **1.1. Compliance Enforcement Authority**

#### **1.2. The RE shall serve as the CEA with the following exceptions:**

- 1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.3** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.4** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

#### **1.3. Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### **1.4. Data Retention**

- 1.4.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### **1.5. Additional Compliance Information**

- 1.5.1** None

### **2. Violation Severity Levels**

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation,  OR  The document is not approved by the senior manager,  OR  Changes to the delegated authority are not documented	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;  AND  changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. (Retired)	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. (Retired)	LOWER	Exceptions to the Responsible Entity’s cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity’s cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. (Retired)	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. (Retired)	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

**E. Regional Variances**

None identified.

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
2		<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets.</p> <p>Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	<p>FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	
3, 4	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-3a
3. **Purpose:** Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability**
  - 4.1. Within the text of Standard CIP-005-3, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity
  - 4.2. The following are exempt from Standard CIP-005-3:
    - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
  - R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
  - R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

- R1.3.** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
- R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.
- R1.5.** Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
- R1.6.** The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
- R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
  - R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
  - R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
  - R2.3.** The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
  - R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
  - R2.5.** The required documentation shall, at least, identify and describe:
    - R2.5.1.** The processes for access request and authorization.
    - R2.5.2.** The authentication methods.
    - R2.5.3.** The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
    - R2.5.4.** The controls used to secure dial-up accessible connections.
  - R2.6.** Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)
- R3.** Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

- R3.1.** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
- R3.2.** Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
- R4.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R4.1.** A document identifying the vulnerability assessment process;
  - R4.2.** A review to verify that only ports and services required for operations at these access points are enabled;
  - R4.3.** The discovery of all access points to the Electronic Security Perimeter;
  - R4.4.** A review of controls for default accounts, passwords, and network management community strings;
  - R4.5.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R5.** Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.
  - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
  - R5.2.** The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
  - R5.3.** The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

## C. Measures

- M1.** The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.
- M5.** The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

## D. Compliance

### 1. Compliance Monitoring Process

**1.1. Compliance Enforcement Authority**

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

**1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

**1.3. Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

**1.4. Data Retention**

**1.4.1** The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.2** The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

**2. Violation Severity Levels (To be developed later.)**

**E. Regional Variances**

None identified.

**Version History**

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		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. Rerwording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## Appendix 1

Requirement Number and Text of Requirement
<p><b>Section 4.2.2</b> Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.</p> <p><b>Requirement R1.3</b> Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).</p>
Question 1 (Section 4.2.2)
<p>What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?</p>
Response to Question 1
<p>In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.</p>
Question 2 (Section 4.2.2)
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
Response to Question 2
<p>The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.</p>
Question 3 (Requirement R1.3)
<p>Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
Response to Question 3
<p>The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</p>
Question 4 (Requirement R1.3)
<p>If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal</p>

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

**Response to Question 4**

In the case where the "endpoint" is defined as logical and is  $\geq$  layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

A. **Introduction**

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-4a
3. **Purpose:** Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability**
  - 4.1. Within the text of Standard CIP-005-4a, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity
  - 4.2. The following are exempt from Standard CIP-005-4a:
    - 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.
    - 4.2.4 In nuclear plants, 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.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. **Requirements**

- R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
  - R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

- R1.2.** For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
- R1.3.** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
- R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.
- R1.5.** Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
- R1.6.** The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
- R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
  - R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
  - R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
  - R2.3.** The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
  - R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
  - R2.5.** The required documentation shall, at least, identify and describe:
    - R2.5.1.** The processes for access request and authorization.
    - R2.5.2.** The authentication methods.
    - R2.5.3.** The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.
    - R2.5.4.** The controls used to secure dial-up accessible connections.
  - R2.6.** Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

- R3.** Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
  - R3.1.** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
  - R3.2.** Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
- R4.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R4.1.** A document identifying the vulnerability assessment process;
  - R4.2.** A review to verify that only ports and services required for operations at these access points are enabled;
  - R4.3.** The discovery of all access points to the Electronic Security Perimeter;
  - R4.4.** A review of controls for default accounts, passwords, and network management community strings;
  - R4.5.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R5.** Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.
  - R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.
  - R5.2.** The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
  - R5.3.** The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

## C. Measures

- M1.** The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.
- M5.** The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

**D. Compliance**

**1. Compliance Monitoring Process**

**1.1. Compliance Enforcement Authority**

**1.2. The RE shall serve as the CEA with the following exceptions:**

- 1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

**1.3. Compliance Monitoring and Enforcement Processes**

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

**1.4. Data Retention**

- 1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.
- 1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

**2. Violation Severity Levels**

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.  OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retired)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

**E. Regional Variances**

None identified.

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s).</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	Revised.
3	12/16/09	<p>Changed CIP-005-2 to CIP-005-3.</p> <p>Changed all references to CIP Version “2” standards to CIP Version “3” standards.</p> <p>For Violation Severity Levels, changed, “To be developed later” to “Developed separately.”</p>	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	<p>Update to conform to changes to CIP-002-4 (Project 2008-06)</p> <p>Update version number from “3” to “4a”</p>
4a	4/19/12	<p>FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	
3a, 4a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	



## Appendix 1

Requirement Number and Text of Requirement
<p><b>Section 4.2.2</b> Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.</p> <p><b>Requirement R1.3</b> Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).</p>
Question 1 (Section 4.2.2)
<p>What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?</p>
Response to Question 1
<p>In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.</p>
Question 2 (Section 4.2.2)
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
Response to Question 2
<p>The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.</p>
Question 3 (Requirement R1.3)
<p>Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
Response to Question 3
<p>The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</p>
Question 4 (Requirement R1.3)
<p>If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are</p>

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

**Response to Question 4**

In the case where the "endpoint" is defined as logical and is  $\geq$  layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

## A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-3
3. **Purpose:** Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
4. **Applicability:**
  - 4.1. Within the text of Standard CIP-007-3, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity.
  - 4.2. The following are exempt from Standard CIP-007-3:
    - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
  - R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

- R1.2.** The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
  - R1.3.** The Responsible Entity shall document test results.
- R2.** Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
  - R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
  - R2.2.** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
  - R2.3.** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
  - R3.1.** The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
  - R3.2.** The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
  - R4.1.** The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
  - R4.2.** The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.
- R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
  - R5.1.** The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.
    - R5.1.1.** The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.



- R7.1.** Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.2.** Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.3.** The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. **(Retired)**
- R8.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R8.1.** A document identifying the vulnerability assessment process;
  - R8.2.** A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
  - R8.3.** A review of controls for default accounts; and,
  - R8.4.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R9.** Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

### C. Measures

- M1.** The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.
- M5.** The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.
- M6.** The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.
- M7.** The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
- M8.** The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.
- M9.** The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

### D. Compliance

#### 1. Compliance Monitoring Process

**1.1. Compliance Enforcement Authority**

- 1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2 ERO for Regional Entity.
- 1.1.3 Third-party monitor without vested interest in the outcome for NERC.

**1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

**1.3. Compliance Monitoring and Enforcement Processes**

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

**1.4. Data Retention**

- 1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2 The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.
- 1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information.**

**2. Violation Severity Levels (To be developed later.)**

**E. Regional Variances**

None identified.

**Version History**

Version	Date	Action	Change Tracking
2		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 and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		<p>Assets within an Electronic Security Perimeter.                  Replaced the RRO with the RE as a responsible entity.                  Rewording of Effective Date.                  R9 changed ninety (90) days to thirty (30) days                  Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-4
3. **Purpose:** Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability:**
  - 4.1. Within the text of Standard CIP-007-4, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity.
  - 4.2. The following are exempt from Standard CIP-007-4:
    - 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 In nuclear plants, 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
    - 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

- R1.1.** The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
- R1.2.** The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
- R1.3.** The Responsible Entity shall document test results.
- R2.** Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
  - R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
  - R2.2.** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
  - R2.3.** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
  - R3.1.** The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
  - R3.2.** The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
  - R4.1.** The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
  - R4.2.** The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.
- R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
  - R5.1.** The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.

- R5.1.1.** The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.
  - R5.1.2.** The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
  - R5.1.3.** The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
- R5.2.** The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
  - R5.2.1.** The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
  - R5.2.2.** The Responsible Entity shall identify those individuals with access to shared accounts.
  - R5.2.3.** Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
- R5.3.** At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
  - R5.3.1.** Each password shall be a minimum of six characters.
  - R5.3.2.** Each password shall consist of a combination of alpha, numeric, and “special” characters.
  - R5.3.3.** Each password shall be changed at least annually, or more frequently based on risk.
- R6.** Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
  - R6.1.** The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
  - R6.2.** The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
  - R6.3.** The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
  - R6.4.** The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
  - R6.5.** The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

- R7.** Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
  - R7.1.** Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
  - R7.2.** Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
  - R7.3.** The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)
- R8.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R8.1.** A document identifying the vulnerability assessment process;
  - R8.2.** A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
  - R8.3.** A review of controls for default accounts; and,
  - R8.4.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R9.** Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

### C. Measures

- M1.** The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.
- M5.** The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.
- M6.** The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.
- M7.** The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
- M8.** The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.
- M9.** The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

#### 1.2. The RE shall serve as the CEA with the following exceptions:

- 1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

- 1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2 The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.
- 1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information.

### 2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, <b>but did not document</b> that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program <b>but</b> did not include one or more of the following:  tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 <b>but</b> did not maintain records as specified in R7.3.  (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 <b>but</b> did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 <b>but</b> did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retired)	LOWER	N/A	N/A	N/A	N/A

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually <b>nor</b> were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

**E. Regional Variances**

None identified.

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
2		<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment and acceptance of risk.</p> <p>Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>R9 changed ninety (90) days to thirty (30) days</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	<p>FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012)</p> <p>Added approved VRF/VSL table to section D.2.</p>	
3, 4	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** System Restoration from Blackstart Resources
2. **Number:** EOP-005-2
3. **Purpose:** Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.
4. **Applicability:**
  - 4.1. Transmission Operators.
  - 4.2. Generator Operators.
  - 4.3. Transmission Owners identified in the Transmission Operators restoration plan.
  - 4.4. Distribution Providers identified in the Transmission Operators restoration plan.
5. **Proposed Effective Date:** Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

## B. Requirements

- R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Time Horizon = Operations Planning]*
  - R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.
  - R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.
  - R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.
  - R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.
  - R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.
  - R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

- R1.7.** Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.
- R1.8.** Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.
- R1.9.** Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.
- R2.** Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Time Horizon = Operations Planning]*
- R3.** Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Time Horizon = Operations Planning]*
  - R3.1.** If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retired)
- R4.** Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Time Horizon = Operations Planning]*
  - R4.1.** Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.
- R5.** Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Time Horizon = Operations Planning]*
- R6.** Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Time Horizon = Long-term Planning]*
  - R6.1.** The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.
  - R6.2.** The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.
  - R6.3.** The capability of generating resources required to control voltages and frequency within acceptable operating limits.
- R7.** Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each

affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Time Horizon = Real-time Operations]*

- R8.** Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Time Horizon = Real-time Operations]*
- R9.** Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Time Horizon = Operations Planning]*
  - R9.1.** The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.
  - R9.2.** A list of required tests including:
    - R9.2.1.** The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.
    - R9.2.2.** The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.
  - R9.3.** The minimum duration of each of the required tests.
- R10.** Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Time Horizon = Operations Planning]*
  - R10.1.** System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.
  - R10.2.** Restoration priorities.
  - R10.3.** Building of cranking paths.
  - R10.4.** Synchronizing (re-energized sections of the System).
- R11.** Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Time Horizon = Operations Planning]*

- R12.** Each Transmission Operator shall participate in its Reliability Coordinator’s restoration drills, exercises, or simulations as requested by its Reliability Coordinator. [*Time Horizon = Operations Planning*]
- R13.** Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. [*Time Horizon = Operations Planning*]
- R14.** Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. [*Time Horizon = Operations Planning*]
- R15.** Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator’s restoration plan within 24 hours following such change. [*Time Horizon = Operations Planning*]
- R16.** Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. [*Time Horizon = Operations Planning*]
- R16.1.** Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.
- R16.2.** Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.
- R17.** Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: [*Time Horizon = Operations Planning*]
- R17.1.** System restoration plan including coordination with the Transmission Operator.
- R17.2.** The procedures documented in Requirement R14.
- R18.** Each Generator Operator shall participate in the Reliability Coordinator’s restoration drills, exercises, or simulations as requested by the Reliability Coordinator. [*Time Horizon = Operations Planning*]

**C. Measures**

- M1.** Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

- M2.** Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.
- M3.** Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.
- M4.** Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.
- M5.** Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.
- M6.** Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.
- M7.** If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.
- M8.** If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.
- M9.** Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.
- M10.** Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.
- M11.** Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.
- M12.** Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

- M13.** Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.
- M14.** Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.
- M15.** Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.
- M16.** Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.
- M17.** Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.
- M18.** Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

#### **D. Compliance**

##### **1. Compliance Monitoring Process**

###### **1.1. Compliance Enforcement Authority**

Regional Entity.

###### **1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

###### **1.3. Compliance Monitoring and Enforcement Processes:**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

###### **1.4. Data Retention**

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

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

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

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

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

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

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

**1.5. Additional Compliance Information**

None.

**2. Violation Severity Levels**

**E. Regional Variances**

None.

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	TBD	R3.1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

**A. Introduction**

- 1. Title:** Coordination of Plans For New Generation, Transmission, and End-User Facilities
- 2. Number:** FAC-002-1
- 3. Purpose:** To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.
- 4. Applicability:**
  - 4.1.** Generator Owner
  - 4.2.** Transmission Owner
  - 4.3.** Distribution Provider
  - 4.4.** Load-Serving Entity
  - 4.5.** Transmission Planner
  - 4.6.** Planning Authority
- 5. (Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

**B. Requirements**

- R1.** The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:
  - 1.1.** Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.
  - 1.2.** Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.
  - 1.3.** Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.
  - 1.4.** Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.
  - 1.5.** Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.
- R2.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days). (Retired)

**C. Measures**

- M1.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider’s documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0\_R1.
- M2.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0\_R2. (Retired)

**D. Compliance**

**1. Compliance Monitoring Process**

**1.1. Compliance Enforcement Authority**

Regional Entity.

**1.2. Compliance Monitoring Period and Reset Timeframe**

Not applicable.

**1.3. Compliance Monitoring and Enforcement Processes:**

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

**1.4. Data Retention**

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

**1.5. Additional Compliance Information**

None

**2. Violation Severity Levels (no changes)**

**E. Regional Differences**

- 1. None identified.

**Version History**

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of “Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

**Standard FAC-002-1 — Coordination of Plans for New Facilities**

---

1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	
---	-----	--	--

**A. Introduction**

- 1. Title:** Facility Ratings Methodology
- 2. Number:** FAC-008-1
- 3. Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
- 4. Applicability**
  - 4.1.** Transmission Owner
  - 4.2.** Generator Owner
- 5. Effective Date:** August 7, 2006

**B. Requirements**

- R1.** The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:
  - R1.1.** A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
  - R1.2.** The method by which the Rating (of major BES equipment that comprises a Facility) is determined.
    - R1.2.1.** The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
    - R1.2.2.** The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.
  - R1.3.** Consideration of the following:
    - R1.3.1.** Ratings provided by equipment manufacturers.
    - R1.3.2.** Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).
    - R1.3.3.** Ambient conditions.
    - R1.3.4.** Operating limitations.
    - R1.3.5.** Other assumptions.
- R2.** The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request. (Retired)
- R3.** If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the

Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

**C. Measures**

- M1.** The Transmission Owner and Generator Owner shall each have a documented Facility Ratings Methodology that includes all of the items identified in FAC-008 Requirement 1.1 through FAC-008 Requirement 1.3.5.
- M2.** The Transmission Owner and Generator Owner shall each have evidence it made its Facility Ratings Methodology available for inspection within 15 business days of a request as follows: (Retired)
  - M2.1** The Reliability Coordinator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Reliability Coordinator Area. (Retired)
  - M2.2** The Transmission Operator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its portion of the Reliability Coordinator Area. (Retired)
  - M2.3** The Transmission Planner shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Transmission Planning Area. (Retired)
  - M2.4** The Planning Authority shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Planning Authority Area. (Retired)
- M3.** If the Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall have evidence that it provided a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

**D. Compliance**

**1. Compliance Monitoring Process**

**1.1. Compliance Monitoring Responsibility**

Regional Reliability Organization

**1.2. Compliance Monitoring Period and Reset Time Frame**

Each Transmission Owner and Generator Owner shall self-certify its compliance to the Compliance Monitor at least once every three years. New Transmission Owners and Generator Owners shall each demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

**1.3. Data Retention**

The Transmission Owner and Generator Owner shall each keep all superseded portions of its Facility Ratings Methodology for 12 months beyond the date of the change in that methodology and shall keep all documented comments on the Facility Ratings Methodology and associated responses for three years. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

**1.4. Additional Compliance Information**

The Transmission Owner and Generator Owner shall each make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

- 1.4.1** Facility Ratings Methodology
- 1.4.2** Superseded portions of its Facility Ratings Methodology that had been replaced, changed or revised within the past 12 months
- 1.4.3** Documented comments provided by a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Authority on its technical review of a Transmission Owner’s or Generator Owner’s Facility Ratings methodology, and the associated responses

**2. Levels of Non-Compliance**

**2.1. Level 1:** There shall be a level one non-compliance if any of the following conditions exists:

- 2.1.1** The Facility Ratings Methodology does not contain a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- 2.1.2** The Facility Ratings Methodology does not address one of the required equipment types identified in FAC-008 R1.2.1.
- 2.1.3** No evidence of responses to a Reliability Coordinator’s, Transmission Operator, Transmission Planner, or Planning Authority’s comments on the Facility Ratings Methodology. **(Retired)**

**2.2. Level 2:** The Facility Ratings Methodology is missing the assumptions used to determine Facility Ratings or does not address two of the required equipment types identified in FAC-008 R1.2.1.

**2.3. Level 3:** The Facility Ratings Methodology does not address three of the required equipment types identified in FAC-008-1 R1.2.1.

**2.4. Level 4:** The Facility Ratings Methodology does not address both Normal and Emergency Ratings ~~or the Facility Ratings Methodology was not made available for inspection within 15 business days of receipt of a request.~~ **(Deleted text retired)**

**E. Regional Differences**

None Identified.

**Version History**

Version	Date	Action	Change Tracking
1	01/01/05	1. Lower cased the word “draft” and “drafting team” where appropriate. 2. Changed incorrect use of certain hyphens (-) to “en dash” (–) and “em dash (—).” 3. Changed “Timeframe” to “Time	01/20/05

**Standard FAC-008-1 — Facility Ratings Methodology**

---

		Frame” and “twelve” to “12” in item D, 1.2.	
1	TBD	R2 and R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

**A. Introduction**

1. **Title:** **Facility Ratings**
2. **Number:** FAC-008-3
3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.
4. **Applicability**
  - 4.1. Transmission Owner.
  - 4.2. Generator Owner.
5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

**B. Requirements**

- R1.** Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. [*Violation Risk Factor: Lower*] [*Time Horizon: Long-term Planning*]
- 1.1.** The documentation shall contain assumptions used to rate the generator and at least one of the following:
- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
  - Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.
- 1.2.** The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- R2.** Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning*]
- 2.1.** The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:
- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
  - A practice that has been verified by testing, performance history or engineering analysis.
- 2.2.** The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:
- 2.2.1.** Equipment Rating standard(s) used in development of this methodology.
  - 2.2.2.** Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
  - 2.2.3.** Ambient conditions (for particular or average conditions or as they vary in real-time).
  - 2.2.4.** Operating limitations.<sup>1</sup>
- 2.3.** A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
- 2.4.** The process by which the Rating of equipment that comprises a Facility is determined.
- 2.4.1.** The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
  - 2.4.2.** The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.
- R3.** Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following:  
*[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*
- 3.1.** The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:
- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
  - One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
  - A practice that has been verified by testing, performance history or engineering analysis.
- 3.2.** The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:
- 3.2.1.** Equipment Rating standard(s) used in development of this methodology.

---

<sup>1</sup> Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

- 3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.
      - 3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).
      - 3.2.4. Operating limitations.<sup>2</sup>
    - 3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.
    - 3.4. The process by which the Rating of equipment that comprises a Facility is determined.
      - 3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.
      - 3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.
- R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)
- R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)
- R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
- R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

---

<sup>2</sup> Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

- 8.1.** As scheduled by the requesting entities:
  - 8.1.1.** Facility Ratings
  - 8.1.2.** Identity of the most limiting equipment of the Facilities
- 8.2.** Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:
  - 8.2.1.** Identity of the existing next most limiting equipment of the Facility
  - 8.2.2.** The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

**C. Measures**

- M1.** Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.
- M2.** Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.
- M3.** Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.
- M4.** Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retired)
- M5.** If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retired)
- M6.** Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).
- M7.** Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.
- M8.** Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

**D. Compliance**

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority**

Regional Entity

1.2. **Compliance Monitoring and Enforcement Processes:**

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

1.3. **Data Retention**

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retired)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. **Additional Compliance Information**

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	<ul style="list-style-type: none"> <li>The Generator Owner’s Facility Rating documentation did not address Requirement R1, Part 1.1.</li> </ul>	The Generator Owner’s Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	<p>The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> <li>2.1.</li> <li>2.2.1</li> <li>2.2.2</li> <li>2.2.3</li> <li>2.2.4</li> </ul>	<p>The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> <li>2.1</li> <li>2.2.1</li> <li>2.2.2</li> <li>2.2.3</li> <li>2.2.4</li> </ul>	<p>The Generator Owner’s Facility Rating methodology did not address all the components of Requirement R2, Part 2.4.</p> <p>OR</p> <p>The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> <li>2.1.</li> <li>2.2.1</li> <li>2.2.2</li> <li>2.2.3</li> <li>2.2.4</li> </ul>	<p>The Generator Owner’s Facility Rating methodology failed to recognize a facility’s rating based on the most limiting component rating as required in Requirement R2, Part 2.3</p> <p>OR</p> <p>The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2:</p> <ul style="list-style-type: none"> <li>2.1</li> <li>2.2.1</li> <li>2.2.2</li> <li>2.2.3</li> <li>2.2.4</li> </ul>
R3	<p>The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> <li>3.1</li> <li>3.2.1</li> </ul>	<p>The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> <li>3.1</li> <li>3.2.1</li> </ul>	<p>The Transmission Owner’s Facility Rating methodology did not address either of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> <li>3.4.1</li> <li>3.4.2</li> </ul>	<p>The Transmission Owner’s Facility Rating methodology failed to recognize a Facility’s rating based on the most limiting component rating as required in Requirement R3, Part 3.3</p> <p>OR</p>

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<ul style="list-style-type: none"> <li>• 3.2.2</li> <li>• 3.2.3</li> <li>• 3.2.4</li> </ul>	<ul style="list-style-type: none"> <li>• 3.2.2</li> <li>• 3.2.3</li> <li>• 3.2.4</li> </ul>	<p>OR</p> <p>The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> <li>• 3.1</li> <li>• 3.2.1</li> <li>• 3.2.2</li> <li>• 3.2.3</li> <li>• 3.2.4</li> </ul>	<p>The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3:</p> <ul style="list-style-type: none"> <li>• 3.1</li> <li>• 3.2.1</li> <li>• 3.2.2</li> <li>• 3.2.3</li> <li>• 3.2.4</li> </ul>
<p>R4 (Retired)</p>	<p>The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.</p>	<p>The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.</p>	<p>The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.</p>	<p>The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)</p>
<p>R5 (Retired)</p>	<p>The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)</p>	<p>The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request.</p> <p>OR</p> <p>The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)</p>	<p>The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request.</p> <p>OR</p> <p>The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)</p>	<p>The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)</p>

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days.  OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1)  OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1)	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1)  OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1)  OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1)  OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1)  OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1)  OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1)  OR The responsible entity provided the required Rating information to the requesting entity, but did so more

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>OR</p> <p>The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>The responsible entity provided the required Rating information to the requesting entity, but did so more than 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)</p>	<p>than 35 calendar days late. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2)</p> <p>OR</p> <p>The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)</p>

E. **Regional Variances**

None.

F. **Associated Documents**

**Version History**

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	TBD	R4 and R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## **Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

---

### **A. Introduction**

- 1. Title:** System Operating Limits Methodology for the Planning Horizon
- 2. Number:** FAC-010-2.1
- 3. Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
- 4. Applicability**
  - 4.1. Planning Authority**
- 5. Effective Date:** April 19, 2010

### **B. Requirements**

- R1.** The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:
  - R1.1.** Be applicable for developing SOLs used in the planning horizon.
  - R1.2.** State that SOLs shall not exceed associated Facility Ratings.
  - R1.3.** Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2.** The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
  - R2.1.** In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.
  - R2.2.** Following the single Contingencies<sup>1</sup> identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
    - R2.2.1.** Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
    - R2.2.2.** Loss of any generator, line, transformer, or shunt device without a Fault.
    - R2.2.3.** Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
  - R2.3.** Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:
    - R2.3.1.** Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

---

<sup>1</sup> The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.



## **Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

- M2.** The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.
- M3.** If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. **(Retired)**

### **D. Compliance**

#### **1. Compliance Monitoring Process**

##### **1.1. Compliance Monitoring Responsibility**

Regional Reliability Organization

##### **1.2. Compliance Monitoring Period and Reset Time Frame**

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

##### **1.3. Data Retention**

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. **(Deleted text retired)**

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

##### **1.4. Additional Compliance Information**

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

**1.4.1** SOL Methodology.

**1.4.2** Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. **(Retired)**

**1.4.3** Superseded portions of its SOL Methodology that had been made within the past 12 months.

**1.4.4** Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

#### **2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)**

**2.1. Level 1:** There shall be a level one non-compliance if either of the following conditions exists:

**2.1.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

**2.1.2** No evidence of responses to a recipient's comments on the SOL Methodology. **(Retired)**

## **Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

---

- 2.2. Level 2:** The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.
- 2.3. Level 3:** There shall be a level three non-compliance if any of the following conditions exists:
  - 2.3.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.
  - 2.3.2** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.
  - 2.3.3** The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.
- 2.4. Level 4:** The SOL Methodology was not issued to all required entities in accordance with R4

**Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

**3. Violation Severity Levels:**

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

**Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

Requirement	Lower	Moderate	High	Severe
	<p>to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but</p>

**Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon**

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
R5 (Retired)	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days.  OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer.  OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

**E. Regional Differences**

- 1.** The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
  - 1.1.** As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
    - 1.1.1** Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.
    - 1.1.2** A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
    - 1.1.3** Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
    - 1.1.4** The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
    - 1.1.5** A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
    - 1.1.6** A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.
    - 1.1.7** The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
  - 1.2.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
    - 1.2.1** All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
    - 1.2.2** Cascading does not occur.
    - 1.2.3** Uncontrolled separation of the system does not occur.
    - 1.2.4** The system demonstrates transient, dynamic and voltage stability.
    - 1.2.5** Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
    - 1.2.6** Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

## Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

- 1.2.7** To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3.** SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
- 1.3.1** Cascading does not occur.
- 1.4.** The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

### Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word “each” from the 1 <sup>st</sup> sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

**A. Introduction**

- 1. Title:** System Operating Limits Methodology for the Operations Horizon
- 2. Number:** FAC-011-2
- 3. Purpose:** To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.
- 4. Applicability**
  - 4.1.** Reliability Coordinator
- 5. Effective Date:** April 29, 2009

**B. Requirements**

- R1.** The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:
  - R1.1.** Be applicable for developing SOLs used in the operations horizon.
  - R1.2.** State that SOLs shall not exceed associated Facility Ratings.
  - R1.3.** Include a description of how to identify the subset of SOLs that qualify as IROLs.
- R2.** The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:
  - R2.1.** In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.
  - R2.2.** Following the single Contingencies<sup>1</sup> identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.
    - R2.2.1.** Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.
    - R2.2.2.** Loss of any generator, line, transformer, or shunt device without a Fault.
    - R2.2.3.** Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.
  - R2.3.** In determining the system's response to a single Contingency, the following shall be acceptable:
    - R2.3.1.** Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

---

<sup>1</sup> The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.



- M1.** The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.
- M2.** The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.
- M3.** If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5 **(Retired)**

## **D. Compliance**

### **1. Compliance Monitoring Process**

#### **1.1. Compliance Monitoring Responsibility**

Regional Reliability Organization

#### **1.2. Compliance Monitoring Period and Reset Time Frame**

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

#### **1.3. Data Retention**

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years.~~ In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. **(Deleted text retired)**

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

#### **1.4. Additional Compliance Information**

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

**1.4.1** SOL Methodology.

**1.4.2** Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. **(Retired)**

**1.4.3** Superseded portions of its SOL Methodology that had been made within the past 12 months.

**1.4.4** Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

### **2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)**

- 2.1. Level 1:** There shall be a level one non-compliance if either of the following conditions exists:
  - 2.1.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.
  - 2.1.2** No evidence of responses to a recipient's comments on the SOL Methodology (Retired)
- 2.2. Level 2:** The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.
- 2.3. Level 3:** There shall be a level three non-compliance if any of the following conditions exists:
  - 2.3.1** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.
  - 2.3.2** The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.
  - 2.3.3** The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.
- 2.4. Level 4:** The SOL Methodology was not issued to all required entities in accordance with R4.

**3. Violation Severity Levels:**

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	<p>provided up to 30 calendar days after the effectiveness of the change.</p>	<p>calendar days or more, but less than 60 calendar days after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>calendar days or more, but less than 90 calendar days after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.</p>	<p>changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change.                      OR                      The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to</p>

Requirement	Lower	Moderate	High	Severe
<p>R5 (Retired)</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.</p>	<p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.</p>	<p>30 calendar days after the effectiveness of the change.</p> <p>The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.</p>

## Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:
  - 1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
    - 1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.
    - 1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7
    - 1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.
    - 1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
    - 1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.
    - 1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.
    - 1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.
  - 1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:
    - 1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.
    - 1.2.2 Cascading does not occur.
    - 1.2.3 Uncontrolled separation of the system does not occur.
    - 1.2.4 The system demonstrates transient, dynamic and voltage stability.
    - 1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.
    - 1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

- 1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.
- 1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:
  - 1.3.1 Cascading does not occur.
- 1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

**Version History**

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed “Cascading Outage” to “Cascading” Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon
2. **Number:** FAC-013-2
3. **Purpose:** To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.
4. **Applicability:**
  - 4.1. **Planning Coordinators**
5. **Effective Date:**

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

## B. Requirements

- R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning* ]
  - 1.1. Criteria for the selection of the transfers to be assessed.
  - 1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).
  - 1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.
  - 1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:
    - 1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.
    - 1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.
    - 1.4.3. System demand.
    - 1.4.4. Current approved and projected Transmission uses.



### C. Measures

- M1.** Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.
- M2.** Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2
- M3.** Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retired)
- M4.** Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.
- M5.** Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.
- M6.** Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

### D. Compliance

#### 1. Compliance Monitoring Process

##### 1.1. Compliance Enforcement Authority

Regional Entity

##### 1.2. Data Retention

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

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods 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 Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

**1.4. Additional Compliance Information**

None

**2. Violation Severity Levels**

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	<p>The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> <li>• Part 1.1</li> <li>• Part 1.2</li> <li>• Part 1.3</li> <li>• Part 1.5</li> </ul> <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> <li>• Part 1.1</li> <li>• Part 1.2</li> <li>• Part 1.3</li> <li>• Part 1.5</li> </ul> <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.</p>	<p>The Planning Coordinator did not have a Transfer Capability methodology.</p> <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology:</p> <ul style="list-style-type: none"> <li>• Part 1.1</li> <li>• Part 1.2</li> <li>• Part 1.3</li> <li>• Part 1.5</li> </ul> <p>OR</p> <p>The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.</p>

<p><b>R2</b></p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.</p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request</p>	<p>The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.</p>	<p>The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation.</p> <p>OR</p> <p>The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.</p>
<p><b>R3</b> <b>(Retired)</b></p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.</p>	<p>The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern.</p> <p>OR</p> <p>The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.</p>

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days.  OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
-----	---	--	--	--

<p><b>R5</b></p>	<p>The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.</p>	<p>The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.</p>	<p>The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.</p>	<p>The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.</p>
<p><b>R6</b></p>	<p>The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.</p>	<p>The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.</p>	<p>The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.</p>	<p>The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.</p>

**E. Regional Variances**

None.

**F. Associated Documents**

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
1	08/01/05	<ol style="list-style-type: none"> <li>1. Changed incorrect use of certain hyphens (-) to “en dash (-).”</li> <li>2. Lower cased the word “draft” and “drafting team” where appropriate.</li> <li>3. Changed Anticipated Action #5, page 1, from “30-day” to “Thirty-day.”</li> <li>4. Added or removed “periods.”</li> </ol>	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	<p>FERC Order issued directing the VRF’s for Requirements R1. and R4. be changed from “Lower” to “Medium.”</p> <p>FERC Order issued correcting the High and Severe VSL language for R1.</p>	
2	TBD	R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** Interchange Confirmation
2. **Number:** INT-007-1
3. **Purpose:** To ensure that each Arranged Interchange is checked for reliability before it is implemented.
4. **Applicability**
  - 4.1. Interchange Authority.
5. **Effective Date:** January 1, 2007

## B. Requirements

- R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:
  - R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).
  - R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retired)
  - R1.3. The following are defined:
    - R1.3.1. Generation source and load sink.
    - R1.3.2. Megawatt profile.
    - R1.3.3. Ramp start and stop times.
    - R1.3.4. Interchange duration.
  - R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

## C. Measures

- M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

## D. Compliance

1. **Compliance Monitoring Process**
  - 1.1. **Compliance Monitoring Responsibility**

Regional Reliability Organization.
  - 1.2. **Compliance Monitoring Period and Reset Time Frame**

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.
  - 1.3. **Data Retention**

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

#### **1.4. Additional Compliance Information**

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

- 1.4.1** Verified by audit at least once every three years.
- 1.4.2** Verified by spot checks in years between audits.
- 1.4.3** Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.
- 1.4.4** Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

- 1.4.5** For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.
- 1.4.6** For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

#### **2. Levels of Non-Compliance**

- 2.1. Level 1:** One occurrence<sup>1</sup> where Interchange-related data was not verified as defined in R1.
- 2.2. Level 2:** Two occurrences where Interchange-related data was not verified as defined in R1.
- 2.3. Level 3:** Three occurrences where Interchange-related data was not verified as defined in R1.
- 2.4. Level 4:** Four or more occurrences where Interchange-related data was not verified as defined in R1.

#### **E. Regional Differences**

None

---

<sup>1</sup> This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

### Version History

Version	Date	Action	Change Tracking
1	TBD	R1.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

**A. Introduction**

- 1. Title:** Coordination of Real-time Activities Between Reliability Coordinators
- 2. Number:** IRO-016-1
- 3. Purpose:** To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.
- 4. Applicability**
  - 4.1. Reliability Coordinator**
- 5. Effective Date:** November 1, 2006

**B. Requirements**

- R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
  - R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
  - R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
    - R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
    - R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.
  - R1.3.** If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.
- R2.** The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. **(Retired)**

**C. Measures**

- M1.** For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

**D. Compliance**

- 1. Compliance Monitoring Process**
  - 1.1. Compliance Monitoring Responsibility**

Regional Reliability Organization
  - 1.2. Compliance Monitoring Period and Reset Time Frame**

The performance reset period shall be one calendar year.

**1.3. Data Retention**

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

**1.4. Additional Compliance Information**

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction’s discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

- 1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

**2. Levels of Non-Compliance**

- 2.1. **Level 1:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.
- 2.2. **Level 2:** Not applicable.
- 2.3. **Level 3:** Not applicable.
- 2.4. **Level 4:** For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

**E. Regional Differences**

None identified.

**Version History**

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to “en dash (–).” 2. Hyphenated “30-day” and “Reliability Coordinator-to-Reliability Coordinator” when used as adjective.	01/20/06

**Standard IRO-016-1 — Coordination of Real-time Activities Between Reliability Coordinators**

---

		<ol style="list-style-type: none"><li>3. Changed standard header to be consistent with standard “Title.”</li><li>4. Added “periods” to items where appropriate.</li><li>5. Initial capped heading “Definitions of Terms Used in Standard.”</li><li>6. Changed “Timeframe” to “Time Frame” in item D, 1.2.</li><li>7. Lower cased all words that are not “defined” terms — drafting team, and self-certification.</li><li>8. Changed apostrophes to “smart” symbols.</li><li>9. Removed comma after word “condition” in item R.1.1.</li><li>10. Added comma after word “expected” in item 1.4, last sentence.</li><li>11. Removed extra spaces between words where appropriate.</li></ol>	
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

**A. Introduction**

- 1. Title:** Nuclear Plant Interface Coordination
- 2. Number:** NUC-001-2
- 3. Purpose:** This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.
- 4. Applicability:**
  - 4.1.** Nuclear Plant Generator Operator.
  - 4.2.** Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:
    - 4.2.1** Transmission Operators.
    - 4.2.2** Transmission Owners.
    - 4.2.3** Transmission Planners.
    - 4.2.4** Transmission Service Providers.
    - 4.2.5** Balancing Authorities.
    - 4.2.6** Reliability Coordinators.
    - 4.2.7** Planning Coordinators.
    - 4.2.8** Distribution Providers.
    - 4.2.9** Load-serving Entities.
    - 4.2.10** Generator Owners.
    - 4.2.11** Generator Operators.
- 5. Effective Date:** April 1, 2010

**B. Requirements**

- R1.** The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]
- R2.** The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements<sup>1</sup> that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]
- R3.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]
- R4.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

---

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

- R4.1.** Incorporate the NPIRs into their operating analyses of the electric system.
- R4.2.** Operate the electric system to meet the NPIRs.
- R4.3.** Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.
- R5.** The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]
- R6.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]
- R7.** Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]
- R8.** Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]
- R9.** The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]
  - R9.1.** Administrative elements: (Retired)
    - R9.1.1.** Definitions of key terms used in the agreement. (Retired)
    - R9.1.2.** Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retired)
    - R9.1.3.** A requirement to review the agreement(s) at least every three years. (Retired)
    - R9.1.4.** A dispute resolution mechanism. (Retired)
  - R9.2.** Technical requirements and analysis:
    - R9.2.1.** Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.
    - R9.2.2.** Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.
    - R9.2.3.** Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.
  - R9.3.** Operations and maintenance coordination:
    - R9.3.1.** Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

- R9.3.2.** Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.
- R9.3.3.** Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.
- R9.3.4.** Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.
- R9.3.5.** Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .
- R9.3.6.** Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.
- R9.3.7.** Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.
- R9.4.** Communications and training:
  - R9.4.1.** Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.
  - R9.4.2.** Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.
  - R9.4.3.** Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.
  - R9.4.4.** Provisions for supplying information necessary to report to government agencies, as related to NPIRs.
  - R9.4.5.** Provisions for personnel training, as related to NPIRs.

### C. Measures

- M1.** The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)
- M2.** The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)
- M3.** Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

- M4.** Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:
  - M4.1** The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)
  - M4.2** The electric system was operated to meet the NPIRs. (Requirement 4.2)
  - M4.3** The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)
- M5.** The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)
- M6.** The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)
- M7.** The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)
- M8.** The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

#### **D. Compliance**

##### **1. Compliance Monitoring Process**

###### **1.1. Compliance Enforcement Authority**

Regional Entity.

###### **1.2. Compliance Monitoring Period and Reset Time Frame**

Not applicable.

###### **1.3. Compliance Monitoring and Enforcement Processes:**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

###### **1.4. Data Retention**

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

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

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

#### **1.5. Additional Compliance Information**

None.

### **2. Violation Severity Levels**

- 2.1. Lower:** Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.
- 2.2. Moderate:** Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.
- 2.3. High:** One or more requirements of R3 through R8 were not met.
- 2.4. Severe:** No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

### **E. Regional Differences**

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.

Therefore the definition of NPLR for Canadian CANDU units will be as follows:

**Nuclear Plant Licensing Requirements (NPLR)** are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

### **F. Associated Documents**

### Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	TBD	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## A. Introduction

1. **Title:** **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**
2. **Number:** PRC-010-0
3. **Purpose:** Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.
4. **Applicability:**
  - 4.1. Load-Serving Entity that operates a UVLS program
  - 4.2. Transmission Owner that owns a UVLS program
  - 4.3. Transmission Operator that operates a UVLS program
  - 4.4. Distribution Provider that owns or operates a UVLS program
5. **Effective Date:** April 1, 2005

## B. Requirements

- R1.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).
  - R1.1.** This assessment shall include, but is not limited to:
    - R1.1.1.** Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.
    - R1.1.2.** Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.
    - R1.1.3.** A review of the voltage set points and timing.
- R2.** The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). **(Retired)**

## C. Measures

- M1.** Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0\_R1.
- M2.** Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0\_R2. **(Retired)**

**D. Compliance**

**1. Compliance Monitoring Process**

**1.1. Compliance Monitoring Responsibility**

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

**1.2. Compliance Monitoring Period and Reset Timeframe**

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

**1.3. Data Retention**

None specified.

**1.4. Additional Compliance Information**

None.

**2. Levels of Non-Compliance**

**2.1. Level 1:** Not applicable.

**2.2. Level 2:** Not applicable.

**2.3. Level 3:** Not applicable.

**2.4. Level 4:** An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0\_R1.1 or an assessment of the UVLS program was not provided.

**E. Regional Differences**

1. None identified.

**Version History**

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

# Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

---

## A. Introduction

1. **Title:** Under-Voltage Load Shedding Program Performance
2. **Number:** PRC-022-1
3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).
4. **Applicability**
  - 4.1. Transmission Operator that operates a UVLS program.
  - 4.2. Distribution Provider that operates a UVLS program.
  - 4.3. Load-Serving Entity that operates a UVLS program.
5. **Effective Date:** May 1, 2006

## B. Requirements

- R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:
  - R1.1. A description of the event including initiating conditions.
  - R1.2. A review of the UVLS set points and tripping times.
  - R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.
  - R1.4. A summary of the findings.
  - R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.
- R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retired)

## C. Measures

- M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.
- M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retired)

## D. Compliance

1. Compliance Monitoring Process
  - 1.1. **Compliance Monitoring Responsibility**  
Regional Reliability Organization.
  - 1.2. **Compliance Monitoring Period and Reset Time Frame**

## Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

One calendar year.

### 1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

### 1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

## 2. Levels of Non-Compliance

**2.1. Level 1:** Not applicable.

**2.2. Level 2:** Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

**2.3. Level 3:** Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

**2.4. Level 4:** Documentation of the analysis of UVLS performance was not provided.

## E. Regional Differences

None identified.

## Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	<ol style="list-style-type: none"><li>1. Removed comma after 2004 in “Development Steps Completed,” #1.</li><li>2. Changed incorrect use of certain hyphens (-) to “en dash” (–) and “em dash (—).”</li><li>3. Lower cased the word “region,” “board,” and “regional” throughout document where appropriate.</li><li>4. Added or removed “periods” where appropriate.</li><li>5. Changed “Timeframe” to “Time Frame” in item D, 1.2.</li></ol>	January 20, 2006
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

## Standard VAR-001-2 — Voltage and Reactive Control

---

### A. Introduction

1. **Title:** Voltage and Reactive Control
2. **Number:** VAR-001-2
3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.
4. **Applicability:**
  - 4.1. Transmission Operators.
  - 4.2. Purchasing-Selling Entities.
  - 4.3. Load Serving Entities.
5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

### B. Requirements

- R1. Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.
- R2. Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
- R3. The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.
  - R3.1. Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.
  - R3.2. For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.
- R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule <sup>1</sup> at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).
- R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider. (Retired)

---

<sup>1</sup> The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

## Standard VAR-001-2 — Voltage and Reactive Control

---

- R6.** The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.
- R6.1.** When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.
- R7.** The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.
- R8.** Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.
- R9.** Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; and controllable load– to support its voltage under first Contingency conditions.
- R9.1.** Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.
- R10.** Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.
- R11.** After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.
- R12.** The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

### C. Measures

- M1.** The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.
- M2.** The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.
- M3.** The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.
- M4.** The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

### D. Compliance

- 1. Compliance Monitoring Process**

## Standard VAR-001-2 — Voltage and Reactive Control

---

### 1.1. Compliance Enforcement Authority

Regional Entity.

### 1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

### 1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

### 1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

### 1.5. Additional Compliance Information

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

## 2. Violation Severity Levels (no changes)

### E. Regional Differences

None identified.

### Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	