

## A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-4
3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. **Applicability:**
  - 4.1. Within the text of Standard CIP-002-4, “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-002-4:
    - 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.
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.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.
- R2.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
  - The Cyber Asset uses a routable protocol within a control center; or,
  - The Cyber Asset is dial-up accessible.
- R3.** Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

## C. Measures

- M1.** The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.
- M2.** The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.
- M3.** The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

- 1.1.1** The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:
- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
  - For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- 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.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

**1.2. Compliance Monitoring and Enforcement Processes**

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

**1.3. Data Retention**

- 1.3.1** The Responsible Entity shall keep documentation required by Standard CIP-002-4 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.
- 1.3.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.4. Additional Compliance Information**

- 1.4.1** None.

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

**E. Regional Variances**

None identified.

**Version History**

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	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. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

## CIP-002-4 - Attachment 1

### Critical Asset Criteria

The following are considered Critical Assets:

- 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.
- 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.
- 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.
- 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.
- 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.
- 1.6. Transmission Facilities operated at 500 kV or higher.
- 1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.
- 1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.
- 1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.
- 1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.
- 1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

- 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.
- 1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.
- 1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

## 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.
- 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).
  - 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).
  - R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
  - 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.
- 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.
  - 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.
- 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.
- 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 (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
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)

## A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-4
3. **Purpose:** Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 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-004-4, “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-004-4:
    - 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. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
  - Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
  - Management support and reinforcement (e.g., presentations, meetings, etc.).
- R2.** Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
- R2.1.** This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.
- R2.2.** Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
- R2.2.1.** The proper use of Critical Cyber Assets;
  - R2.2.2.** Physical and electronic access controls to Critical Cyber Assets;
  - R2.2.3.** The proper handling of Critical Cyber Asset information; and,
  - R2.2.4.** Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.
- R2.3.** The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
- R3.** Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.
- The personnel risk assessment program shall at a minimum include:
- R3.1.** The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
  - R3.2.** The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
  - R3.3.** The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.
- R4.** Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
- R4.1.** The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

- R4.2.** The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

**C. Measures**

- M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.
- M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

**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 personnel risk assessment documents in accordance with federal, state, provincial, and local laws.
- 1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 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.

- 1.4.3** 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.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause...”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06
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>Reference to emergency situations.</p> <p>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.</p> <p>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.</p> <p>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to “Critical Cyber Assets”.</p> <p>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3		Update version number from -2 to -3	
3	12/16/09	Approved by 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)

## 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.

- 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 (Developed separately.)**

**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	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	<p>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>	
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>

## Appendix 1

<b>Requirement Number and Text of Requirement</b>
<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>
<b>Question 1 (Section 4.2.2)</b>
<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>
<b>Response to Question 1</b>
<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>
<b>Question 2 (Section 4.2.2)</b>
<p>Is the communication link physical or logical? Where does it begin and terminate?</p>
<b>Response to Question 2</b>
<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>
<b>Question 3 (Requirement R1.3)</b>
<p>Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?</p>
<b>Response to Question 3</b>
<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>
<b>Question 4 (Requirement R1.3)</b>
<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 — Physical Security of Critical Cyber Assets
2. **Number:** CIP-006-4c
3. **Purpose:** Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c 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-006-4c, “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-006-4c:
    - 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. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
  - R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

- R1.2.** Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
- R1.3.** Processes, tools, and procedures to monitor physical access to the perimeter(s).
- R1.4.** Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
- R1.5.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
- R1.6.** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
  - R1.6.1.** Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
  - R1.6.2.** Continuous escorted access of visitors within the Physical Security Perimeter.
- R1.7.** Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
- R1.8.** Annual review of the physical security plan.
- R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
  - R2.1.** Be protected from unauthorized physical access.
  - R2.2.** Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
- R3.** Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.
- R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
  - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
  - Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
  - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R5.** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the



Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
  - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.
- R6.** Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
  - Video Recording: Electronic capture of video images of sufficient quality to determine identity.
  - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
- R7.** Access Log Retention — The Responsible Entity shall retain physical 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.
- R8.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
- R8.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
  - R8.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.
  - R8.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

### C. Measures

- M1.** The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.
- M2.** The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.
- M3.** The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.
- M4.** The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

- M5.** The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.
- M6.** The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.
- M7.** The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.
- M8.** The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

## **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 documents other than those specified in Requirements R7 and R8.2 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** The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.
- 1.5.2** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

**2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)****E. Regional Variances**

None identified.

**Version History**

<b>Version</b>	<b>Date</b>	<b>Action</b>	<b>Change Tracking</b>
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2  Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3  Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term “Responsible Entity” was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1.  Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	<p>FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4.</p> <p>Updated version number from -3/-4 to -3c/-4c.</p>	

## Appendix 1

<b>Requirement Number and Text of Requirement</b>
<p>R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:</p> <p style="padding-left: 40px;">R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.</p>
<b>Question</b>
<p>If a completely enclosed border cannot be created, what does the phrase, “to control physical access” require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?</p> <p>Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?</p>
<b>Response</b>
<p>For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are “physical in nature.” The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed (“six-wall”) border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p>

## Appendix 2

### Interpretation of Requirement R1.1.

**Request:** *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

**Interpretation:**

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a “six-wall” border.

**CIP-006-1 — Requirement 1.1** requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

**R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**

**R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**

**CIP-006-1 — Additional Compliance Information 1.4.4** identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

**1.4. Additional Compliance Information**

**1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.**

## Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

### Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, “time of access” mean logging when the person entered the facility or does it mean logging the entry/exit time and “length” of time the person had access to the critical asset?*

### Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term “time of access” refers to the time an authorized individual enters the physical security perimeter.

### Requirement Number and Text of Requirement

- R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:**
- R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.**
  - R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.**
  - R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.**

## 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.
- 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 (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.	

		<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)

## A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-4
3. **Purpose:** Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 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-008-4, “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-008-4:
    - 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. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
  - R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

- R1.2.** Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.
- R1.3.** Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
- R1.4.** Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
- R1.5.** Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
- R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.
- R2.** Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

### C. Measures

- M1.** The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.
- M2.** The Responsible Entity shall make available all documentation as specified in Requirement R2.

### 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 documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for 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** The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

**1.5.2** The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

**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. Reworking of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by 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)



## A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets
2. **Number:** CIP-009-4
3. **Purpose:** Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 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-009-3, “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-009-4:
    - 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. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
  - R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
  - R1.2. Define the roles and responsibilities of responders.

- R2.** Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.
- R3.** Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.
- R4.** Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.
- R5.** Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

### **C. Measures**

- M1.** The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.
- M2.** The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.
- M3.** The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.
- M4.** The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.
- M5.** The Responsible Entity shall make available its documentation of testing of backup media 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.
- 1.2.2** 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 documentation required by Standard CIP-009-4 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**

**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. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers 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)