

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-002-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14)

Description of Current Draft:

This version of Standard CIP-002 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-002-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-002-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-1
3. **Purpose:** NERC Standards CIP-002 through CIP-009 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. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

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 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 a risk-based assessment.

4. **Applicability:**
 - 4.1. Within the text of Standard CIP-002, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-002:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

- R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
 - R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
 - R1.2.** The risk-based assessment shall consider the following assets:
 - R1.2.1.** Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
 - R1.2.2.** Transmission substations that support the reliable operation of the Bulk Electric System.
 - R1.2.3.** Generation resources that support the reliable operation of the Bulk Electric System.
 - R1.2.4.** Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
 - R1.2.5.** Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
 - R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.
 - R1.2.7.** Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.
- R2.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.
- R3.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
 - R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
 - R3.2.** The Cyber Asset uses a routable protocol within a Control Center; or,
 - R3.3.** The Cyber Asset is dial-up accessible.
- R4.** Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 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

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

- M1.** The risk-based assessment methodology documentation as specified in Requirement R1.
- M2.** The list of Critical Assets as specified in Requirement R2.
- M3.** The list of Critical Cyber Assets as specified in Requirement R3.
- M4.** The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year
- 1.3.2** The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

- 1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

- 2.1 Level 1:** The risk assessment has not been performed annually.
- 2.2 Level 2:** The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.
- 2.3 Level 3:** The list of Critical Assets or Critical Cyber Assets does not exist.
- 2.4 Level 4:** The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-003-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14)

Description of Current Draft:

This version of Standard CIP-003 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-003-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-003-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-1
3. **Purpose:** Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-003, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-003:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

- 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 through CIP-009, including provision for emergency situations.

- 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

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

- M1.** Documentation of the Responsible Entity's 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.** Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.
- M3.** Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.
- M4.** Documentation of the Responsible Entity's information protection program as specified in Requirement R4.
- M5.** The access control documentation as specified in Requirement R5.
- M6.** The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

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

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

- 2.4.1 No cyber security policy exists; or,
- 2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,
- 2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-004-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-004 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-004-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-004-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-1
3. **Purpose:** Standard CIP-004 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 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-004, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-004:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-004:

- R1.** Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access 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, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
- R2.1.** This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
- R2.2.** Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, 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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such 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.
- 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

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:

- M1.** Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.
- M2.** Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.
- M3.** 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.** 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 Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.
- 1.3.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004 from the previous full calendar year.
- 1.3.3** The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

- 1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1** Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,
- 2.1.2** Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,
- 2.1.3** Personnel risk assessment program exists, but documentation of that program does not exist; or,
- 2.1.4** List(s) of personnel with their access control rights is available, but has not been reviewed and updated as required.
- 2.1.5** One personnel risk assessment is not updated at least every seven years, or for cause; or,
- 2.1.6** One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.

2.2. Level 2:

- 2.2.1** Awareness program does not exist or is not implemented; or,
- 2.2.2** Training program exists, but does not address the requirements identified in Standard CIP-004; or,
- 2.2.3** Personnel risk assessment program exists, but assessments are not conducted as required; or,
- 2.2.4** One instance of personnel termination (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.

2.3. Level 3:

- 2.3.1** Training program exists, but has not been reviewed and updated at least annually; or,
- 2.3.2** A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,
- 2.3.3** List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.

2.4. Level 4:

- 2.4.1 No documented training program exists; or,
- 2.4.2 No documented personnel risk assessment program exists; or,
- 2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-005-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-005 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-005-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-005-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-1
3. **Purpose:** Standard CIP-005 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 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-005, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-005:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date: June 1, 2006**

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

- 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.
 - R1.5.** Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
 - 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 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 Requirement R4.

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

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.
- 1.3.2** The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.
- 1.3.3** The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

- 1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.
- 1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1** All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,
- 2.1.2** Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

- 2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,
 - 2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.
- 2.2. Level 2:**
- 2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,
 - 2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,
 - 2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.
- 2.3. Level 3:**
- 2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Assets not within the defined Electronic Security Perimeter(s); or,
 - 2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,
 - 2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or
 - 2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,
 - 2.3.5 Electronic Access Monitoring:
 - 2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,
 - 2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,
 - 2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.
- 2.4. Level 4:**
- 2.4.1 No documented Electronic Security Perimeter exists; or,
 - 2.4.2 No records of access exist; or,
 - 2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,
 - 2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,
 - 2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-006-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-006 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-006-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-006-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security - Physical Security of Critical Cyber Assets
2. **Number:** CIP-006-1
3. **Purpose:** Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-006, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-006:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date: June 1, 2006**

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

- 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.
- R1.2.** Processes to identify all 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.** Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
 - R1.5.** Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
 - R1.6.** Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
 - R1.7.** Process for updating the physical security plan within ninety calendar days 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.** Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.
 - R1.9.** Process for ensuring that the physical security plan is reviewed at least annually.
- R2.** 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:
- R2.1.** 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.
 - R2.2.** 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.
 - R2.3.** Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
 - R2.4.** Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R3.** 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. One or more of the following monitoring methods shall be used:

- R3.1.** 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.
- R3.2.** Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.
- 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.
- R5.** 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.
- R6.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:
 - R6.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
 - R6.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.
 - R6.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

- M1.** The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.
- M2.** Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.
- M3.** Documentation identifying the methods for monitoring physical access as specified in Requirement R3.
- M4.** Documentation identifying the methods for logging physical access as specified in Requirement R4.

- M5. Access logs as specified in Requirement R5.
- M6. Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1 Regional Reliability Organizations for Responsible Entities.
- 1.1.2 NERC for Regional Reliability Organization.
- 1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.
- 1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

- 1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.
- 1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.
- 1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.
- 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.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,
- 2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,
- 2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,
- 2.1.4 Physical access logs are retained for a period shorter than ninety days; or,
- 2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity’s total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity’s total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity’s total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-007-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-007 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-007-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-007-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Systems Security Management
2. **Number:** CIP-007-1
3. **Purpose:** Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-007, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-007:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

- 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, 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 and document 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 or an acceptance of risk.
- R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document 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 or an acceptance of risk.
- 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 or an acceptance of risk.
 - 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 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 Requirement R5 and Standard CIP-004 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.
- 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 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.
 - 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 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

- M1.** Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.
- M2.** Documentation as specified in Requirement R2.
- M3.** Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

- M4.** Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.
- M5.** Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.
- M6.** Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.
- M7.** Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
- M8.** Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.
- M9.** Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

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

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or
- 2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,
- 2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,
- 2.1.4 Any one of:
 - Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
 - A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
 - Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

- 2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,
- 2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

- 2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,
- 2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

- 2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,
- 2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.
- 2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-008-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-008 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-008-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-008-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-1
3. **Purpose:** Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability**
 - 4.1. Within the text of Standard CIP-008, “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 Reliability Organizations.
 - 4.2. The following are exempt from Standard CIP-008:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

- R1.** Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. 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 incident response teams, 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 ninety 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 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

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

- M1.** The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan
- M2.** All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.
- 1.3.2** The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

- 1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.
- 1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.
- 1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.
- 1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Levels of Noncompliance

- 2.1. **Level 1:** A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.
- 2.2. **Level 2:**
 - 2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,
 - 2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,
 - 2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.
- 2.3. **Level 3:**
 - 2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,
 - 2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.
- 2.4. **Level 4:** A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP-009-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)
6. Review comments to draft 2 and revise as needed
7. Post Draft 3 for 45-day public comment period (May 9 – June 23, 2005)
8. Review comments to draft 3 and revise as needed (June 24, 2005 – January 15, 2006)
9. Post for 30-day pre-ballot review (January 16 – February 14, 2006)

Description of Current Draft:

This version of Standard CIP-009 addresses comments received in response to draft 3. It represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), to ensure that levels of noncompliance are auditable and correctly matched to the requirements, to clarify the requirements, and to eliminate redundancy between the standards.

Future Development Plan:

1. Host a webcast for NERC's ballot body	January 31, 2006
2. First ballot of Standard CIP-009-1	February 15 – February 24, 2006
3. Respond to comments	February 25 – March 13, 2006
4. Post for recirculation ballot	March 14 – March 24, 2006
5. 30-day posting before board adoption	March 25 – April 24, 2006
6. Board adopts Standard CIP-009-1	May 2, 2006
7. Effective date	June 1, 2006

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
- Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter: The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets
2. **Number:** CIP-009-1
3. **Purpose:** Standard CIP-009 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 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.
4. **Applicability:**
 - 4.1. Within the text of Standard CIP-009, “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 Reliability Organizations
 - 4.2. The following are exempt from Standard CIP-009:
 - 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
 - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
 - 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
5. **(Proposed) Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009:

- 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 ninety calendar days of the change.
- 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

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:

- M1.** Recovery plan(s) as specified in Requirement R1.
- M2.** Records documenting required exercises as specified in Requirement R2.
- M3.** Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.
- M4.** Documentation regarding backup and storage of information as specified in Requirement R4.
- M5.** Documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

- 1.1.1** Regional Reliability Organizations for Responsible Entities.
- 1.1.2** NERC for Regional Reliability Organization.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

- 1.3.1** The Responsible Entity shall keep documentation required by Standard CIP-009 from the previous full calendar year.
- 1.3.2** The Compliance Monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

- 1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.
- 1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

- 2.1.1** Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,
- 2.1.2** Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.

2.2. Level 2:

- 2.2.1** Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,
- 2.2.2** Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.

2.3. Level 3:

- 2.3.1** Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,
- 2.3.2** Recovery plan(s) exist, but have not been exercised during the previous full calendar year.

2.4. Level 4:

- 2.4.1** No recovery plan(s) exist; or,
- 2.4.2** Backup of information required to successfully restore Critical Cyber Assets does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking