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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–002–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–002–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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 Assets

2. **Number:** CIP–002–1

Purpose: Standards CIP-002 through CIP-009 provide a cyber security framework identifying and assisting with the protection of Critical Cyber Assets to ensure reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

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

This standard requires the identification and enumeration of the Critical Cyber Assets that support the reliable operation of the Bulk Electric System identified through the application of a risk-based assessment procedure.

3. **Applicability:**

3.1. Within the text of this standard, “Responsible Entity” shall mean:

3.1.1 Reliability Coordinator.

3.1.2 Balancing Authority.

3.1.3 Interchange Authority.

3.1.4 Transmission Service Provider.

3.1.5 Transmission Owner.

3.1.6 Transmission Operator.

3.1.7 Generator Owner.

3.1.8 Generator Operator.

3.1.9 Load Serving Entity.

3.1.10 NERC.

3.1.11 Regional Reliability Organizations.

3.2. The following entities are exempt from this standard:

3.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

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

4. **(Proposed) Effective Date:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Critical Assets — The Responsible Entity shall identify its Critical Assets and maintain a current list of all Critical Assets identified. The Responsible Entity shall review, and as necessary, update the list of Critical Assets annually, or within ninety calendar days of the addition of, removal of, or modification to any Critical Asset.

R1.1. Required Critical Assets

R1.1.1. Control centers and backup control centers performing the functions listed in the Applicability section of this standard.

R1.1.2. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers. These shall include telemetering, monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange.

R1.1.3. Transmission substation elements in the direct transfer path associated with an Interconnection Reliability Operating Limit (IROL).

R1.1.4. Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.

R1.1.5. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.

R1.1.6. Systems, equipment and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.1.7. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of shedding 300 MW or more.

R1.1.8. Special Protection Systems whose misoperation can negatively affect elements associated with an IROL.

R1.2. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets due to unique system configurations or other unique requirements. The risk-based assessment must include a description of the assessment including the determining criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, additional Critical Assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System.

R2. Critical Cyber Assets — The Responsible Entity shall identify the Critical Cyber Assets associated with each Critical Asset listed in Requirement R1. The Responsible Entity shall review and, as necessary, update the list of Critical Cyber Assets annually, or within ninety calendar days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset. For the purpose of this standard, Critical Cyber Assets, as defined, have the following characteristics:

R2.1. The Cyber Asset uses a routable protocol, unless the Cyber Asset is within a substation or generation station where a routable protocol does not extend beyond the physical boundary of the facility; or,

R2.2. The Cyber Asset is dial-up accessible.

R3. Annual Review — A senior manager or delegate(s) shall review and approve annually the list of Critical Assets and the list of Critical Cyber Assets. A signed and dated record of the senior manager or delegate(s)'s review and approval of the list of Critical Assets and the list of Critical Cyber Assets shall be maintained. Based on the process in R1 and R2, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. The list of Critical Assets identified in R1 and documentation of the risk-based assessment, including a description of the methodology (the determining criteria, potential impacts, and evaluation procedure) and supporting documentation.

M2. An approved list of Critical Cyber Assets as identified under Requirement R2.

M3. Signed and dated records of the senior manager or delegate(s)'s review and approval of the list of Critical Assets and of the list of Critical Cyber Assets.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep the following data from the previous full calendar year:

- Signed lists of critical assets, and records of updates and annual reviews.
- Signed lists of critical cyber assets, and records of updates and annual reviews.
- Documentation of all risk assessments.

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

1.4. Additional Compliance Information

None specified.

2. Levels of Non-Compliance

2.1 Level 1: The required documents (as listed in M1, M2 and M3) exist, but lists of Critical Assets and Critical Cyber Assets have not been updated with changes within ninety calendar days.

2.2 Level 2: The required documents (as listed in M1, M2 and M3) exist, but have not been approved, updated or reviewed in the last calendar year.

2.3 Level 3: One or more documents are missing.

2.4 Level 4: No documents 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 1301) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–003–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–003–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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.

Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP–003–1

3. **Purpose:** This standard requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

4.1. Within the text of this standard, "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 entities are exempt from this standard:

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 are exempt from complying with this standard.

5. **(Proposed) Effective Date:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Cyber Security Policy — Responsible Entities shall document and implement a cyber security policy that defines a structure of relationships and decision-making processes that identify and represent management's commitment and ability to secure its Critical Cyber Assets.

R1.1. The Responsible Entity's cyber security policy shall, at a minimum, address NERC CIP-002 through CIP-009 Standards.

R1.2. The Responsible Entity shall verify that its written cyber security policy is available as needed.

R1.3. The Responsible Entity shall review the structure of internal corporate relationships and processes related to this program at least annually to ensure that the existing relationships and processes continue to provide the appropriate level of accountability and that management is continually engaged in the process.

R1.4. The Responsible Entity's cyber security policy shall be reviewed and approved annually.

R2. Leadership — The Responsible Entity shall assign a senior manager with responsibility for leading and managing the entity's implementation and adherence of the NERC CIP-002 through CIP-009 Standards.

R2.1. The designated senior manager shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the designated senior manager must be documented within thirty calendar days of the effective date.

R2.3. This person, or a designated delegate(s), must authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate.

R3.1. Exceptions to the cyber security policy must be reviewed and approved annually by senior management to ensure the exceptions are still required and valid.

R3.2. Documented exceptions to the aforementioned cyber security policy must include any compensating measures or risk acceptance.

R3.3. The date of the review shall be documented.

R4. Information Protection — The Responsible Entity shall document and implement a program to identify, classify, and protect information relating to Critical Cyber Assets.

R4.1. The Responsible Entity shall identify and protect information relating to Critical Cyber Assets, regardless of media type. At minimum this shall include procedures, Critical Asset inventories, Critical Cyber Asset network topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information.

R4.2. The Responsible Entity shall classify information related to Critical Cyber Assets based on sensitivity.

R4.3. The Responsible Entity shall at least annually assess and document: the Critical Cyber Asset information identification and classification controls; the cyber security protection controls; and, compliance with the documented processes.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to information associated with Critical Cyber Assets.

R5.1. The Responsible Entity shall maintain a list of personnel who are responsible for authorizing access to Critical Cyber Assets.

R5.1.1. Logical or physical access to Critical Cyber Assets may only be authorized by designated personnel.

R5.1.2. The list of designated personnel responsible for authorizing access to Critical Cyber Assets shall identify each designated person by name, title, business phone and list of systems/applications for which they are responsible to authorize access.

R5.1.3. The list of designated personnel responsible for authorizing access shall be verified at least annually.

R5.2. Responsible Entities shall review at least annually the access privileges to information associated with Critical Cyber Assets to confirm the access privileges are correct and that they correspond with the entity's needs and the appropriate roles and responsibilities.

R5.3. The Responsible Entity shall review and document at least annually the processes for controlling access privileges.

R6. Change Control — The Responsible Entity shall establish and document a methodical process of change control for modifying or replacing any Critical Cyber Asset hardware or software.

R6.1. The Responsible Entity shall review its processes for managing change to and testing of Critical Cyber Assets at least annually.

R6.2. The Responsible Entity shall implement an approval authority responsible for formal sign-off on testing results prior to a system (new or modified) being promoted to operate in a production environment.

R6.3. The Responsible Entity shall implement supporting configuration management activities to identify, control and report any changes to hardware and software components of Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. The Responsible Entity's written and approved cyber security policy, relationships, and processes, including annual reviews and updates.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's senior manager responsible for its adherence to the cyber security policy.

M3. The Responsible Entity's written and approved exceptions, including compensating measures or risk acceptance and annual reviews.

M4. The Responsible Entity's written and approved program for the identification, classification and protection of information associated with Critical Cyber Assets, including documentation of annual assessments.

M5. The Responsible Entity's written and approved policy for the management of access to information, including all required lists and documentation of annual reviews.

M6. The Responsible Entity's written and approved processes of change control and configuration management, documented controls for testing and assessment of hardware and software, and documentation of annual reviews.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep data 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

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. Refer to Requirement R3 of this standard. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 A senior manager was not designated for ten or more calendar days, but less than thirty calendar days during a calendar year; or,

2.1.2 A written cyber security policy exists, but has not been reviewed in the last three calendar years; or,

2.1.3 Deviations from requirements or written cyber security policy have not been documented within thirty calendar days of the exception; or,

2.1.4 A program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been reviewed in the previous full calendar year.

2.2. Level 2:

2.2.1 A senior manager was not designated for thirty or more calendar days, but less than sixty calendar days, during a 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 have not been reviewed within the last calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager was not designated for sixty or more calendar days, but less than ninety calendar days, during a calendar year; or,

2.3.2 Roles and/or responsibilities of personnel with access to Critical Cyber Assets have not been defined and documented; or,

2.3.3 The list of designated personnel responsible to authorize access to logical or physical Critical Cyber Assets does not exist; or,

2.3.4 The controls for the testing and assessment of new or replacement systems and software patches/changes have not been documented.

2.4. Level 4:

2.4.1 A senior manager was not designated for more than ninety calendar days during a calendar year; or,

2.4.2 No cyber security policy exists; or,

2.4.3 No identification and classification program exists; or,

2.4.4 An internal corporate relationship structure with defined processes related to this standard does not exist; or,

2.4.5 Access authorizations have not been reviewed within the last calendar year; or,

2.4.6 Access revocations/changes are not authorized and/or documented.

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 1303) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–004–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–004–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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:** This standard requires that personnel having authorized access to Critical Cyber Assets, including contractors and service vendors, have a higher level of risk assessment, training, security awareness, than personnel not provided access. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

4.1. Within the text of this standard, “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 entities are exempt from this standard:

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 are exempt from complying with this standard.

5. **(Proposed) Effective Date:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Awareness — The Responsible Entity shall establish, maintain, and document its security awareness program to ensure personnel subject to the standard 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 (e.g., presentations, all-hands meetings, etc.).

R2. Training — The Responsible Entity shall establish, maintain, and document its annual cyber security training program and shall review and update the program annually.

R2.1. This program will ensure that all personnel having authorized access to Critical Cyber Assets, including contractors and service vendors are trained.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by this standard, and include, at a minimum, the following required items:

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;

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 —

R3.1. The Responsible Entity shall, consistent with the Responsible Entity's legal and human resources requirements, subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented personnel risk assessment process prior to granting authorized access to Critical Cyber Assets.

R3.2. The Responsible Entity shall conduct a documented personnel risk assessment, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, of all personnel covered by this standard prior to their being granted access to Critical Cyber Assets.

R3.2.1. A minimum of identity verification (e.g., Social Security Number verification in the U.S.) and five year criminal check is required. Responsible Entities may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2.2. The Responsible Entity shall update personnel risk assessments at least every five years or for cause.

R3.2.3. The Responsible Entity shall document the results of personnel risk assessment of all personnel having authorized access to Critical Cyber Assets, including contractors and service vendors.

R4. Access — The Responsible Entity shall maintain lists of all authorized personnel with access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets within the security perimeter(s).

R4.1. The Responsible Entity shall review the list of all authorized personnel who have access to Critical Cyber Assets quarterly, and update that list within seven calendar days of any change of personnel with access to Critical Cyber Assets, or any change in the access rights of such personnel.

R4.2. The Responsible Entity shall revoke physical and electronic access within 24 hours for any personnel terminated for cause and within seven calendar days for any personnel who have a change in status where they are no longer allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. Documentation of the Responsible Entity's security awareness program program and its quarterly reinforcement.

M2. Documentation of the Responsible Entity's cyber security training program, its annual review, and training records of the Responsible Entity's authorized personnel who have access to Critical Cyber Assets.

M3. Documentation of the personnel risk assessment process and that the process has been applied to authorized personnel who have access to Critical Cyber Assets.

M4. The list(s) of the Responsible Entity's authorized personnel, documentation of the list's annual review and update, and evidence that access revocation has occurred as needed within the specified timeframes.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

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 for the duration of employee employment plus three years and contractor and service vendor records for the duration of their engagement plus three years.

1.3.2 The Responsible Entity shall keep all other documentation required by this standard for the previous full calendar year.

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

1.4. Additional Compliance Information

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.

Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 List(s) of personnel with their access control rights list is available, but has not been updated or reviewed for more than three months but less than six months; or,

2.1.2 One instance of personnel termination (employee, contractor or service provider) in which access and the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or,

2.1.3 Personnel risk assessment program exists, but documentation of that program either does not exist or reveals that the program does not meet the requirements of this standard, or,

2.1.4 Training program exists, but records of training either do not exist or reveal personnel who have access to Critical Cyber Assets were not trained as required; or,

2.1.5 Awareness program exists, but not applied consistently or within the minimum required period of quarterly reinforcement.

2.2. Level 2:

2.2.1 Access control document(s) exist, but have not been updated or reviewed for more than six months but less than 12 months; or,

2.2.2 More than one but not more than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or,

2.2.3 Training program exists, but does not address one or more of the requirements identified in this standard, or,

2.2.4 Awareness program does not exist or is not implemented, or,

2.2.5 Personnel risk assessment program exists, but is not consistently applied.

2.3. Level 3:

2.3.1 List of personnel with their access control rights exists, but does not include service vendors; and contractors; or,

2.3.2 More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or,

2.3.3 A personnel risk assessment program exists, but is not documented; or,

2.3.4 Training documents exist, but do not cover two or more of the specified items; or,

2.3.5 The training program documentation was not reviewed and updated at least annually; or,

2.3.6 Adverse employment actions are not consistent with the responsible entity's legal and human resources practices for hiring and retention of employees or contractors.

2.3.7 Update personnel risk assessment not conducted at least every five years, or for cause.

2.4. Level 4:

2.4.1 No training program addressing Critical Cyber Assets exists.

2.4.2 No personnel risk assessment program exists.

2.4.3 No documentation 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 1304) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–005–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–005–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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

2. **Number:** CIP–005–1

3. **Purpose:** This standard 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. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

   4.1. Within the text of this standard, "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 this standard:

   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 are exempt from complying with this standard.

5. **(Proposed) Effective Date:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Electronic Security Perimeter —The Responsible Entity shall identify the Electronic Security Perimeter(s) surrounding its Critical Cyber Assets 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 dial-up accessible Critical Cyber Assets that use non-routable protocols, 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 perimeters shall not be considered part of the security perimeter. However, end points of these communication links within the security perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Non-critical Cyber Assets within the defined Electronic Security Perimeter(s) shall be subject to the requirements of this standard.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the same protections as Critical Cyber Assets.

R1.6. The Responsible Entity shall maintain documents depicting the Electronic Security Perimeter(s), all interconnected Critical and non-Critical Cyber Assets within the security perimeter(s), all electronic access points to the security perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points. The entity shall ensure that all Critical Cyber Assets have been identified and are within the documented Electronic Security Perimeter(s). The Responsible Entity shall also ensure that all non-Critical Cyber Assets within the Electronic Security Perimeter(s) have been identified.

R2. Electronic Access Controls — The Responsible Entity shall implement the organizational, technical, and procedural controls to permit or deny electronic access at all electronic access points to the Electronic Security Perimeter(s). These access controls of the Electronic Security Perimeter(s) shall use an access control model that denies access by default unless explicit access permissions are specified.

R2.1. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only those ports and services that are required for normal and emergency operations, and monitoring of Cyber Assets within the Electronic Security Perimeter.

R2.1.1. All other ports and services at these access points, including those used for testing purposes, shall be disabled prior to production usage.

R2.1.2. The Responsible Entity shall document the status and configuration of all ports and services enabled on all access points to the Electronic Security Perimeter(s).

R2.2. The Responsible Entity shall maintain documents identifying the organizational, technical and procedural controls for electronic access and their implementation for each electronic access point to the Electronic Security Perimeter(s). The documents shall identify and describe:

R2.2.1. The access request and authorization process implemented for that control.

R2.2.2. The authentication methods used.

R2.2.3. A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003, as well as personnel access requirements defined in Standard CIP-004, and ongoing supporting documentation (for example, access request and authorization documents, review checklists) verifying that these policies and controls have been implemented.

R2.3. The Responsible Entity shall maintain a documented procedure for securing dial-up access to the Electronic Security Perimeter(s). The documentation shall describe controls implemented to secure these connections.

R2.4. Where external interactive access into the Electronic Security Perimeter is implemented, the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.

External interactive access is any request for access to the Electronic Security Perimeter that requires human interaction and that originates from any point outside of the Electronic Security Perimeter.

Strong procedural or technical controls, in the context of this standard, include any additional procedural or technical authentication measure to augment static user name and password, or any authentication measure which implements one-time use passwords.

R2.5. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access Control — The Responsible Entity shall implement and document the controls for logging authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement monitoring controls at the single access point at the dial-up device, where technically feasible.

R3.2. Where monitoring controls have not been implemented or have only been implemented partially, the Responsible Entity shall implement procedures to verify authorized access to the protected Critical Cyber Asset on a periodic basis, as determined and documented by the Responsible Entity's risk-based assessment.

R3.3. At least every ninety calendar days, the Responsible Entity shall review access logs for unauthorized access or attempts.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1 A document identifying the vulnerability assessment process;

R4.2 Scanning to verify that only ports and services required for normal and emergency operations at these access points are enabled;

R4.3 The discovery of modem(s) connected to the Electronic Security Perimeter;

R4.4 A review of controls for default accounts, passwords and network management community strings; and,

R4.5 Documentation of the results and of an action plan to remediate or mitigate vulnerabilities identified in the assessment.

R5. Documentation Review and Maintenance —

R5.1. The Responsible Entity shall ensure that all documentation required by this standard reflect current configurations and processes and shall review the documents and procedures referenced in this standard at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. Documents depicting the Electronic Security Perimeter(s), all Critical and non-Critical Cyber Assets within the Electronic Security Perimeter(s), and all electronic access points to the security perimeter(s).

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), including:

M2.1 Documentation of the enabled network ports configuration for all access points to each Electronic Security Perimeter.

M2.2 Documentation, for each access point, on the controls implemented, including:

M2.2.1 The access request and authorization process;

M2.2.2 Authentication method(s);

M2.2.3 The periodic review process for authorization rights, as well as business records documenting the conduct of reviews.

M2.3 Documentation of the dial-up access controls.

M2.4 Documentation of strong technical or procedural controls implemented for external interactive access to the Electronic Security Perimeter(s).

M2.5 Documentation of appropriate use banners and business records of their implementations.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s), as well as logs and business records verifying that these controls have been implemented.

M3.1 Documentation of the monitoring procedures for dial-up accessible access points to the Electronic Security Perimeter.

M3.2 Documentation of the procedures used to verify authorized access to the protected Critical Cyber Asset on a periodic basis.

M3.3 Business records documenting the review of access logs to determine unauthorized access or attempts.

M4. Documentation of the Responsible Entity’s annual vulnerability assessment identified in R4.

M4.1 The Responsible Entity’s vulnerability documentation will include at a minimum that the vulnerability assessment addressed open ports and services, modems and review for default accounts, passwords and network management community strings.

M4.2 The documentation shall include a record of the results of the annual vulnerability assessment, remediation plans for all vulnerabilities that are found, and the execution status of the plan.

M5. Documentation Review and Maintenance

M5.1 Documentation of required reviews.

M5.2 Documentation of changes.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep records (for example, access logs, firewall logs, intrusion detection logs) for a minimum of ninety calendar days.

1.3.2 The Responsible Entity shall keep other documents and records required by this standard from the previous full calendar year.

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

1.4. Additional Compliance Information

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. 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 Document(s) exist, but have not been updated within ninety calendar days of any changes; or,

2.1.2 Aggregate interruptions in the monitoring capability over a full calendar year exist for more than six hours, but less than twenty-four hours; or,

2.1.3 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 Document(s) exist, but have not been updated or reviewed in the last twelve months; or,

2.2.2 Aggregate interruptions in the monitoring capability over a full calendar year exist for one calendar day or more, but for less than seven calendar days; 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 for the last full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there is no verification that all Critical and non-Critical Cyber Assets are within the perimeter(s) described; or,

2.3.2 Document(s) exist confirming that only necessary network ports and services have been enabled, but no records documenting annual reviews exist; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified, or the document(s) do not identify or describe access controls for one or more access points; or,

2.3.4 Electronic Access Monitoring:

2.3.4.1 Access not monitored to any access point to the Electronic Security Perimeter for seven calendar days or more;

2.3.4.2 Access logs exist, but have not been reviewed within the past 90 calendar days; or,

2.3.5 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 perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 No records of monitoring exist; 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 no records exist of any vulnerability assessment of the Electronic Security Perimeter(s).

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 (??)
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 1305) (January 17, 2004)
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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–006–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–006–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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:** This standard is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

4.1. Within the text of this standard, "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 this standard:

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:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Physical Security Plan — The Responsible Entity shall create, document, and maintain a physical security plan. The physical security plan shall address, at a minimum, the following:

R1.1. Clearly identified Physical Security Perimeters(s) and all physical access points. Where a six wall boundary cannot be established, the Responsible Entity shall deploy measures such as a security enclosure (a cage/safe/cabinet system that controls physical access to the critical cyber assets).

R1.2. Measures to control access at all access points of the perimeter(s), and to protect the Critical Cyber Assets within them.

R1.3. Processes, tools and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the use of access cards, including card loss, visitor passes, and inappropriate uses, such as piggybacking and card sharing.

R1.5. Processes for reviewing access authorization requests, revocation of access authorization, and periodic review for each physical access control implemented under R3.

R2. Documentation Review — The Responsible Entity shall review its physical security plan at least annually, and update the plan within ninety calendar days of any modification to any components.

R3. Physical Access Controls **—** The Responsible Entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s). The Responsible Entity shall implement one or more of the following physical access methods:

R3.1. 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.

R3.2. Special locks: These may include locks with non-reproducible keys, or magnetic locks that can be operated remotely, or double locks of a Man-trap.

R3.3. Security personnel: Personnel responsible for controlling physical access twenty-four hours a day. These personnel shall reside on-site or at a central monitoring station.

R3.4. Other authentication devices: Biometric, keypad, token, or other devices that are used to control access to the Critical Cyber Assets through personnel authentication.

R4. Monitoring Physical Access — The Responsible Entity shall implement the organizational, 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, using one or more of the following monitoring methods:

R4.1. Closed-circuit television (CCTV): Video surveillance to capture and record images of activity in or around the secure perimeter or facility access point.

R4.2. Alarm systems: Systems that indicate a door or gate has been opened without authorization. These alarms must report back to a central monitoring station. Examples include card key alarm systems, door contacts, window contacts, and motion sensors.

R4.3. Human observation of access points: Monitoring of physical access points by on-site security personnel stationed at entrances.

R5. Logging Physical Access — The Responsible Entity shall implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods. Methods shall record sufficient information to uniquely identify individuals:

R5.1. Manual logging: A log book or sign-in sheet, or other record of physical access accompanied by human observation or remote verification.

R5.2. Computerized logging: Electronic logs produced by the selected access control and monitoring method.

R5.3. Video recording: Electronic capture of video images.

R6. Access Log Retention and Review — The responsible entity shall retain physical access logs for at least 90 calendar days. Unauthorized access attempts shall be reviewed every two months.

R7. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems operate properly.

R7.1. The Responsible Entity shall annually test and maintain all physical security mechanisms implemented to ensure proper operation.

R7.2. The Responsible Entity shall maintain a record of outage duration (from time of discovery to time of repair) of access controls, logging and monitoring.

R7.3. The Responsible Entity shall maintain documentation of testing and maintenance for a period of one full calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. The physical security plan as outlined in R1.

M2. Records documenting the review and any update of the physical security plan, as required in R2.

M3. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter.

M4. Documentation identifying the methods for monitoring physical access.

M5. Documentation identifying the methods for logging physical access.

M6. Access logs and records documenting log retention and the review of unauthorized access attempts.

M7. Records documenting maintenance and testing of the physical security system, as required in R7.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep security logs for ninety calendar days.

1.3.2 The Responsible Entity shall keep all other documents specified in this standard for 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 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. Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

1.4.2 The Responsible Entity may not take exception in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.3 For generating facilities where the electronic security perimeter extends to areas that cannot be physically secured for safety reasons, the Responsible Entity shall, at a minimum, secure the control room, and related computer rooms that support the control function and contain Critical Cyber Assets. The Responsible Entity shall document exceptions along with compensating controls.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1. Required documentation exists, but has not been updated within ninety calendar days of a modification to the physical security plan or any of its components; or,

2.1.2. Access control, monitoring and logging exists, but aggregate interruptions in system or data availability over a full calendar year exist for more than seven calendar days, but less than thirty calendar days.

2.2. Level 2:

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

2.2.2. Access control, monitoring and logging exists, but aggregate interruptions in system or data availability over a full calendar year exist for more than thirty calendar days, but less than ninety calendar days.

2.3. Level 3:

2.3.1. More than one required record does not exist; or,

2.3.2. Required documentation exists, but has not been updated or reviewed in the last twelve months; or,

2.3.3. Access control, monitoring and logging exists, but aggregate interruptions in system or data availability over a full calendar year exist for more than ninety calendar days.

2.4. Level 4:

2.4.1. No access control, or no monitoring, or no logging of access exists, as required; or,

2.4.2. No maintenance or no testing of physical security systems has been performed within the previous full calendar year; or,

2.4.3. No physical security plan 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 1306) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–007–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–007–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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:**
This standard requires that Responsible Entities have system security controls in force to detect, deter, and prevent the failure or compromise of critical functions performed by Critical Cyber Assets caused by mistake, misuse, or malicious activity. This standard 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). This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

4.1. Within the text of this standard, "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 entities are exempt from this standard:

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:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Non-Critical Cyber Assets — Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. The Responsible Entity shall document all non-critical Cyber Assets within the Electronic Security Perimeter(s).

R2. Test Procedures — The Responsible Entity shall use its documented cyber security test procedures for all new systems and significant changes to existing Critical Cyber Assets. For purposes of this standard, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, version upgrades to operating systems, applications, and database platforms, or other third-party software and firmware.

R2.1. The Responsible Entity shall maintain a document identifying cyber security test procedures. These procedures shall be implemented in a manner that precludes adversely affecting the production system and operation.

R2.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R2.3. The Responsible Entity shall maintain records of test results.

R3. Ports and Services — The Responsible Entity shall document the status and configuration of all ports and services available on Cyber Assets inside the Electronic Security Perimeter(s). (Requirements for scanning ports and services at the Electronic Security Perimeter are covered in CIP-005.) The Responsible Entity shall enable only those ports and services required for normal and emergency operations. All other ports and services, including those used for testing purposes, must be disabled prior to production usage of the Cyber Assets inside the Electronic Security Perimeter(s). In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall use and document compensating measure(s) to help mitigate risk exposure.

R4. Security Patch Management — The Responsible Entity shall establish and document a security patch management program for tracking, evaluating, testing, and installation of applicable cyber security software patches for cyber assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document the assessment of security patches and upgrades for applicability within 30 calendar days of availability.

R4.2. Following established configuration management and change control processes, the Responsible Entity shall document the implementation of patches. In the case where the patch is not installed, the Responsible Entity shall document any compensating measure(s) or acceptance of risk.

R5. Anti-Virus Software — The Responsible Entity shall use anti-virus software and related file integrity monitoring tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters.

R5.1. The Responsible Entity shall document the assessment of anti-virus and integrity monitoring tool signatures for applicability within 30 calendar days of availability.

R5.2. Following established configuration management and change control processes, the Responsible Entity shall document the implementation of anti-virus and integrity monitoring tool signatures. In the case where anti-virus and integrity monitoring tools are not installed, the Responsible Entity shall document any compensating measure(s) or acceptance of risk.

R6. Account Management — The Responsible Entity shall establish, implement, and document account management methods that enforce access authentication and accountability of user activity, and minimize the risk of unauthorized system access.

R6.1. The Responsible Entity shall ensure that administrator, individual, and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R6.1.1. Whenever technically possible, end-user and system administrator accounts shall be created, managed, and monitored on an individual user per account basis.

R6.1.2. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel in CIP-003, R5.

R6.1.3. The Responsible Entity shall establish methods, processes and procedures that generate logs of sufficient detail to create historical audit trails of individual user account activity at any moment in time.

R6.1.4. Field devices that do not enforce electronic access control must have physical protections to appropriately control access to said devices.

R6.1.5. A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003, as well as personnel access requirements defined in Standard CIP-004, and ongoing supporting documentation (for example, access request and authorization documents, review checklists) verifying that these policies and controls have been implemented.

R6.2. The Responsible Entity shall implement a policy to manage the scope and acceptable use of the administrator, shared, and other generic account privileges including factory default accounts.

R6.2.1. The process shall include the removal, disabling, or renaming of these accounts where possible. For those accounts that must remain, passwords shall be changed prior to putting any system into service.

R6.2.2. Where technically supported, individual accounts shall be used (in contrast to a shared account).

R6.2.3. The Responsible Entity shall identify those individuals with access to shared accounts.

R6.2.4. Where individual accounts are not supported, the Responsible Entity shall have a policy for managing the appropriate use of shared 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 staff changes (for example, change in assignment or termination).

R6.2.5. The policy shall support a compliance audit of all account usage to an individually named person, that is, individually named user accounts or personal registration for any generic accounts.

R6.3. In the absence of strong authentication methods (e.g. use of multi-factor access controls, digital certificates, or bio-metrics) the Responsible Entity shall require and utilize passwords as technically feasible.

R6.3.1. Each password shall be a minimum of six characters.

R6.3.2. Each password shall consist of a combination of alpha, numeric, and special characters.

R6.3.3. Each password shall be changed annually or more frequently, based on risk.

R7. Security Status Monitoring — The Responsible Entity shall ensure 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.

R7.1. The Responsible Entity shall implement and document the organizational, technical, and procedural controls for monitoring for security events on Cyber Assets within the Electronic Security Perimeter.

R7.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R7.3. The Responsible Entity shall maintain logs of system events related to cyber security in sufficient detail to enable a root-cause analysis.

R7.4. The Responsible Entity shall retain logs for 90 calendar days.

R7.5. The Responsible Entity shall review logs of system events related to cyber security and maintain business records documenting review of logs.

R8. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Critical Cyber Assets.

R8.1. Prior to the disposal of Critical Cyber Assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval.

R8.2. Prior to redeployment of Critical Cyber Assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval.

R8.3. The Responsible Entity shall maintain business records documenting that Critical Cyber Assets were disposed of or redeployed in accordance with documented procedures.

R9. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R9.1. A document identifying the vulnerability assessment process;

R9.2. A review and verification that only ports and services required for normal and emergency operations of the Critical Cyber Asset are enabled;

R9.3. A review of controls for default accounts; and,

R9.4. An action plan to define, execute, and document the results of remediation or mitigation of vulnerabilities identified in the assessment.

R10. Documentation Review and Maintenance — The Responsible Entity shall review the documents referenced in this standard at least annually and shall update these documents within thirty calendar days of any modification of the systems or controls.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. The list of non-critical Cyber Assets identified in R1.

M2. Documentation of the Responsible Entity's security test procedures.

M2.1 The Responsible Entity shall maintain a document identifying cyber security test procedures.

M2.2 Documentation to support that testing is performed in a manner reflecting the production environment.

M2.3 The Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion of changes to Critical Cyber Assets.

M3. Records documenting the status/configuration of all ports and services on Critical Cyber Assets inside the Electronic Security Perimeter(s), as well as any compensating measures taken to mitigate risk exposure.

M4. Documentation and business records of the Responsible Entity's security patch management program, as identified in R4.

M5. Documentation and records of the Responsible Entity's anti-virus software program as identified in R5.

M6. Documentation and records of the Responsible Entity's account management program as identified in R6.

M7. Documentation and records of the Responsible Entity's security status monitoring program as identified in R7.

M8. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Critical Cyber Assets.

M9. Documentation and records of the Responsible Entity's annual vulnerability assessment as identified in R9 of all Cyber Assets within the Electronic Security Perimeters(s).

M10. Records documenting the annual review of the documents referenced in this standard, and that updates have been made to these documents within thirty calendar days of any modification of the systems or controls.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all data 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.

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.

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 System security controls are in place, but fail to document one of the measures (M1-M10) of this standard; or,

2.1.2 Any one of the documented system security controls has not been reviewed in the previous full calendar year; or,

2.1.3 Any one of the documented systems security controls has not been updated within 30 calendar days of any changes to the system security controls; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year;
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days;
- Security patches and upgrades have not been assessed for applicability within 30 calendar days of availability;
- Anti-virus and integrity monitoring tool signatures have not been assessed for applicability within 30 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-M10) of this standard; or,

2.2.2 Any one of the documented system security controls has not been reviewed in the previous 16 calendar months; or,

2.2.3 Any one of the documented system security controls has not been updated within 60 calendar days of any changes to the system security controls; or,

2.2.4 Any two of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year;
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days;
- Security patches and upgrades have not been assessed for applicability within 30 calendar days of availability;
- Anti-virus and integrity monitoring tool signatures have not been assessed for applicability within 30 calendar days of availability.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M10) of this standard; or,

2.3.2 Any one of the documented system security controls has not been reviewed in the previous 20 calendar months; or,

2.3.3 Any one of the documented system security controls has not been updated within 90 calendar days of any changes to the system security controls; or,

2.3.4 Any three of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year;
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days;
- Security patches and upgrades have not been assessed for applicability within 30 calendar days of availability;
- Anti-virus and integrity monitoring tool signatures have not been assessed for applicability within 30 calendar days of availability.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M10) of this standard; or,

2.4.2 Any one of the documented system security controls has not been reviewed in the previous two calendar years; or,

2.4.3 Any one of the documented system security controls has not been updated within 120 calendar days of any changes to the system security controls; or,

2.4.4 All of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year;
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days;
- Security patches and upgrades have not been assessed for applicability within 30 calendar days of availability;
- Anti-virus and integrity monitoring tool signatures have not been assessed for applicability within 30 calendar days of availability.

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 1307) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–008–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–008–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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:** This standard ensures the identification, classification, response and reporting of Cyber Security Incidents. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability**

   4.1. Within the text of this standard, "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 entities are exempt from this standard:

   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 CIP–002, identify that they have no Critical Cyber Assets.

5. **(Proposed) Effective Date:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain an accurate and adequate Cyber Security Incident response plan.

R1.1. The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents in accordance with cyber event criteria defined in NERC's Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP).

R1.2. The Responsible Entity shall define Cyber Security Incident response actions, including roles and responsibilities of incident response teams, incident handling procedures, escalation, and communication plans.

R1.3. The Responsible Entity shall report Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC) in accordance with reporting criteria defined in the IAW SOP. The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary.

R1.4. The Responsible Entity shall review the Cyber Security Incident response plan at least annually and shall update the plan within ninety calendar days of any changes.

R1.5. The Cyber Security Incident response plan must be tested at least annually.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep documentation related to Cyber Security Incidents reportable per R1.1 for three calendar years. This documentation must include, at a minimum, the following:

R2.1. System and application log file entries.

R2.2. Video and/or physical access records.

R2.3. Documented records of investigations and analysis performed.

R2.4. Records of any action taken including any recovery actions initiated.

R2.5. Records of all Cyber Security Incidents and subsequent reports submitted to the ES ISAC.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. Documentation of the Responsible Entity’s Cyber Security Incident response plan, and records documenting the annual review and test of the plan, as defined in R1.

M2. All documentation per R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all required documentation relating to reportable Cyber Security Incidents for three calendar years.

1.3.2 The Responsible Entity shall keep all other required documentation specified in this standard for 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 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. Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

1.4.2 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.3 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:

2.1.1 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 updated or 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 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC in accordance with the IAW SOP; or,

2.2.4 Records related to Cyber Security Incidents were not maintained for three calendar years, or are incomplete.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements R1.1, R1.2, and R1.3 of this standard; or,

2.3.2 Two or more reportable Cyber Security Incidents have occurred but were not reported to the ES ISAC in accordance with the IAW SOP.

2.4. Level 4:

2.4.1 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 1308) (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)

Description of Current Draft:

The current draft addresses comments received in response to draft 2 and represents significant work by the drafting team to ensure consistency across the suite of Cyber Security Standards (CIP-002-1 through CIP-009-1), match requirements to measures, and eliminate redundancy between the standards.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. WebEx/conference call on Draft 3	June 1, 2005
2. Review comments and prepare final version for balloting	June 24-July 21, 2005
3. Post final draft for 30-day pre-ballot period	July 22–August 21, 2005
4. First ballot of Standard CIP–009–1	August 22–31, 2005
5. Respond to comments	September 1-15, 2005
6. Post for recirculation ballot	September 16-26, 2005
7. 30-day posting before board adoption	September 27-October 26, 2005
8. Board adopts Standard CIP–009–1	November 1, 2005
9. Effective date	November 1, 2005

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: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

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

Critical Cyber Assets: Those 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 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:** This standard 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. This standard should be read as part of a group of standards numbered CIP-002 through CIP-009.

4. **Applicability:**

4.1. Within the text of this standard, “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 this standard:

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:** November 1, 2005

B. Requirements

The Responsible Entity shall comply with the following requirements of this standard:

R1. Recovery Plans — The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets. The recovery plan shall address at a minimum the following:

R1.1. Specify the required 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. Recovery plan(s) shall reflect any changes or lessons learned as a result of an exercise or at any other time as required. An exercise can range from a paper drill to a full operational and physical change over.

R3. Change Control — The recovery plan(s) shall be updated to reflect changes to the plan(s) and 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 secure storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare chips or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable. Testing can be completed off site.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of this standard:

M1. Documentation of the recovery plan(s) along with the events or conditions that would activate the recovery plan(s).

M1.1 Documentation of the required responses to events or conditions of varying duration and severity that would activate the recovery plan.

M1.2 Documented roles and responsibilities of responders.

M2. Records documenting that an exercise has been performed in the previous full calendar year.

M3. Documentation of changes to the recovery plan(s) as appropriate, records documenting that changes have been communicated to personnel responsible for the activation and implementation of recovery plans.

M4. Documentation and implementation of processes and procedures for backup and secure storage of information required to successfully restore Critical Cyber Assets.

M5. Records documenting that recoverability of information stored on computer media has been tested in the previous full calendar year.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation for three calendar years.

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

1.4. Additional Compliance Information

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. 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 Recovery plan(s) exist and are exercised, but do not identify the types of events that necessitate the activation of the recovery plan(s); or,

2.1.2 Recovery plan(s) do not address roles and responsibilities of responsible personnel.

2.2. Level 2:

2.2.1 Recovery plan(s) exist, but have not been reviewed and updated during the previous full calendar year; or,

2.2.2 Documented processes and procedures for the backup and secure 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 computer media for a prolonged period of time to ensure that the information is recoverable has not been performed at least annually; or,

2.3.2 Records of reviews and updates have not been kept for three calendar years.

2.4. Level 4:

2.4.1 No recovery plan(s) exist; or,

2.4.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year; or,

2.4.3 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