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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1302 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–002–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–002–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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

3. Purpose: This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid 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 control 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, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Assets are identified by the application of a risk-based assessment procedure on the operation of the interconnected bulk electric system.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list of Critical Assets is then the basis to identify a list of associated Critical Cyber Assets that must be protected by this standard.

R1.1. Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of 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 such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control, and real-time information exchange. Those Critical Assets include the following:

R1.1.1. Control centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities.

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

R1.1.3. Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL)

R1.1.4. Generating resources under control of a common 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 associated with 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 load shedding 300 MW or greater.

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

R1.1.9. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure.

R2. The Responsible Entity shall identify the critical Cyber Assets associated with each Critical Asset listed in section R1. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics:

R2.1. The Cyber Asset uses a routable protocol, or

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

R2.3. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter

R3. Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets.

R4. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall maintain its approved list of Critical Assets as identified in R1.

M2. The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.

M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R3 and all other Cyber Assets as identified under Requirement R3.

M4. The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, M2, and M3 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset.

M5. A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained.

M6. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (1) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.

1.3. Data Retention

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.3.1 Documentation of the approved list of Critical Assets,

1.3.2 Documentation depicting the risk-based assessment methodology used to identify its Critical Assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure,

1.3.3 Documentation of the approved list of Critical Cyber Assets, and

1.3.4 Documentation of the senior management official's approval of both the Critical Asset list and the critical Cyber Asset list.

1.4. Additional Compliance Information

Not specified

2. Levels of Non-Compliance

2.1. Level 1: The required documents exist, but have not been updated with known changes within thirty (30) calendar days.

2.2. Level 2: The required documents exist, but have not been approved, updated or reviewed in the last calendar year.

2.3. Level 3: One or more document(s) missing.

2.4. Level 4: No document(s) exist.

E. Regional Differences

1. None

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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1301 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions		Anticipated Date
1.	Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2.	Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3.	Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4.	First ballot of Standard CIP–003–1	July 1–10, 2005
5.	Respond to comments, post for recirculation ballot	July 21–31, 2005
6.	30-day posting before board adoption	August 1–31, 2005
7.	Board adopts Standard CIP–003–1	September 1, 2005
8.	Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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 is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

   Critical business and operational functions performed by Cyber Assets affecting the bulk electric system necessitate having security management controls. This section defines the minimum security management controls that the Responsible Entity must have in place to protect Critical Cyber Assets.

   Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

4. **Applicability**

   When used within the text of this standard, "Responsible Entity" shall mean:

   4.1. Reliability Coordinator

   4.2. Balancing Authority

   4.3. Interchange Authority

   4.4. Transmission Service Provider

   4.5. Transmission Owner

   4.6. Transmission Operator

   4.7. Generator Owner

   4.8. Generator Operator

   4.9. Load Serving Entity

   4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

   Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets are exempt from complying with this standard.

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

B. Requirements

R1. The Responsible Entity shall create and maintain a cyber security policy that addresses the requirements of this standard and the governance of the cyber security controls.

R2. The Responsible Entity shall document and implement a program for the protection of critical information associated with Critical Cyber Assets.

R2.1. The Responsible Entity shall identify all information, regardless of media type, related to the entity's Critical Cyber Assets whose compromise could impact the reliability

and/or availability of the bulk electric system for which the entity is responsible. This includes procedures, Critical Asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents must be protected as well.

R2.2. The Responsible Entity shall categorize information related to Critical Cyber Assets to aid personnel with access to this information in determining what information can be disclosed to unauthorized personnel as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization.

R2.3. Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity.

R3. The Responsible Entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation and adherence of the cyber security standard. This person, or designated delegate, must authorize any deviation or exception from the requirements of this standard. Any such deviation or exception and its authorization must be documented.

The Responsible Entity shall also define the roles and responsibilities of Critical Cyber Asset owners, custodians, and users. Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.

R4. Responsible Entities shall define and document a structure of relationships and decision-making processes that identify and represent executive level management's ability to direct and control the entity in order to secure its Critical Cyber Assets. This governance process must include:

R4.1. Responsible Entities shall identify the controls for testing and assessment of new or replacement systems and software patches/changes. Responsible entities shall designate approving authorities that will formally authorize and document that a system has passed testing criteria. The approving authority shall be responsible for verifying that a system meets minimal security configuration standards prior to the system being promoted to operate in a production environment.

R4.2. The Responsible Entity shall establish a Change Control Process that provides a controlled environment for modifying all hardware and software for Critical Cyber Assets. The process should include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process should modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets.

R5. The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.

R5.1. The Responsible Entity shall maintain a list of personnel who are responsible to authorize access to Critical Cyber Assets. Logical or physical access to Critical Cyber Assets may only be authorized by the personnel responsible to authorize access to those assets. All access authorizations must be documented.

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

R5.3. Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented.

C. Measures

M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets.

M2. The Responsible Entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years.

M3. The Responsible Entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.

M4. The Responsible Entity shall review all authorized deviations or exemptions at least annually and shall document the extension or revocation of any reviewed authorized deviation or exemption.

M5. The Responsible Entity shall review the information security protection program at least annually.

M6. The Responsible Entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually.

M7. The Responsible Entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the categorization level assigned to that information.

M8. The Responsible Entity shall assess the critical cyber information identification and categorization procedures to ensure compliance with the documented processes at least annually.

M9. The Responsible Entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information.

M10. The current senior management official responsible for the cyber security program shall be identified by name, title, business phone, business address, and date of designation.

M11. Changes to the current senior management official must be documented within 30 calendar days of the effective date.

M12. The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually.

M13. 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 executive level management is continually engaged in the process.

M13.1 The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment.

M13.2 Change Control and Configuration Management — The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets. The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to their Critical Cyber Assets.

M14. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to Critical Cyber Assets to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.

M15. The list of designated personnel responsible to authorize access to Critical Cyber Assets shall identify each designated person by name, title, business phone, business address, date of designation, and list of systems/applications they are responsible to authorize access for. The list of authorizers shall be reviewed for accuracy at least annually.

M16. The Responsible Entity shall review the processes for access privileges, suspension and termination of user accounts. This review shall be documented. The process shall be periodically reassessed in order to ensure compliance with policy at least annually.

M17. The Responsible Entity shall ensure that any authorized change in user access to Critical Cyber Assets is documented. Documentation shall be reviewed at least annually to ensure compliance with entities' documented access control processes.

M18. The Responsible Entity shall review user access rights to confirm access is still required at least annually.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.3.1 Written cyber security policy;

1.3.2 The name, title, business address, and business phone number of the current designated senior management official and the date of his or her designation.

1.3.3 Documentation of justification for any deviations or exemptions.

1.3.4 Documented review results of this standard and mitigation strategies for the information security protection program. Review results will be kept for a minimum of 3 years.

1.3.5 The list of approving authorities for access to critical cyber information assets.

1.3.6 The name(s) of the designated approving authority(s) responsible for authorizing systems suitable for production.

1.4. Additional Compliance Information

Not specified

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 A current senior management official was not designated for less than 30 calendar days during a calendar year; or

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

2.1.3 Deviations from requirements or written cyber security policy are not documented within 30 calendar days of the deviation, or exception, or

2.1.4 An information security protection program exists but has not been reviewed in the last calendar year, or

2.1.5 Processes to protect information associated with Critical Cyber Assets have not been reviewed in the last calendar year.

2.2. Level 2:

2.2.1 A current senior management official was not designated for 30 or more calendar days, but less than 60 calendar days during a calendar year, or

2.2.2 Access to critical cyber information has not been assessed within the last calendar year, or

2.2.3 An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or

2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been kept current and has not been reviewed within the last calendar year.

2.3. Level 3:

2.3.1 A current senior management official was not designated for 60 or more calendar days, but less than 90 calendar days during a calendar year, or

2.3.2 Deviations to policy are not documented or authorized by the current senior management official or delegate responsible for the cyber security program, or

2.3.3 Roles and/or responsibilities are not clearly and distinctly defined, or

2.3.4 Controls for the testing and assessment of new or replacement systems and software patches/changes have not been identified or the list of designated approving authorities is not maintained and up to date.

2.4. Level 4:

2.4.1 A current senior management official was not designated for more than 90 calendar days during a calendar year; or

2.4.2 No cyber security policy exists, or

2.4.3 No information security program exists, or

2.4.4 Roles and responsibilities have not been defined, or

2.4.5 Executive management has not been engaged in the cyber security program, or

2.4.6 No corporate governance program exists, or

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

2.4.8 There is no authorizing authority to validate systems that are to be promoted to production, or

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

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

E. Regional Differences

1. None

Version History

Version	Date	Action	Change Tracking

R6.

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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1303 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–004–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–004–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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 is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

Personnel having authorized access to Critical Cyber Assets, as defined by this standard, are given a higher level of trust, by definition, and are required to have a higher level of screening, training, security awareness, and record retention of such activity, than personnel not provided access.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

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

R1. Awareness — The Responsible Entity shall develop, maintain, and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices.

R2. Training — The Responsible Entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will ensure that all personnel having authorized access to Critical Cyber Assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these Critical Assets.

R3. Records — The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request.

R4. Personnel Risk Assessment — The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to being granted authorized access to Critical Assets.

C. Measures

M1. Awareness — The Responsible Entity shall develop and maintain awareness programs designed to maintain and promote sound security practices in the application of the standards, to include security awareness reinforcement using one or more of the following mechanisms on at least a quarterly basis:

M1.1 Direct communications (e.g., emails, memos, computer based training, etc.);

M1.2 Security reminders (e.g., posters, intranet, brochures, etc.);

M1.3 Management support (e.g., presentations, all-hands meetings, etc.).

M2. Training — The Responsible Entity shall develop and maintain a company-specific cyber security annual training program that includes, at a minimum, the following required items:

M2.1 The cyber security policy;

M2.2 Physical and electronic access controls to Critical Cyber Assets;

M2.3 The proper release of Critical Cyber Asset information;

M2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

M3. Records — The Responsible Entity shall develop and maintain records to adequately document compliance with this standard.

M3.1 The Responsible Entity shall maintain documentation of all personnel who have access to Critical Cyber Assets and the date of completion of their training.

M3.2 The Responsible Entity shall maintain documentation that it has reviewed and updated its training program annually.

M4. Personnel Risk Assessment — The Responsible Entity shall:

M4.1 Maintain a list 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).

M4.2 Review the document referred to in measure M4.1 of this standard quarterly, and update the listing within seven calendar days of any substantive change of personnel.

M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).

M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized access to Critical Cyber Assets in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. A minimum of identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check is required. 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.

M4.5 The Responsible Entity shall ensure that adverse employment actions are consistent with the Responsible Entity's legal and human resources practices for hiring and retention of employees or contractors.

M4.6 The Responsible Entity shall conduct update screenings at least every five years or for cause.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement.

1.4. Additional Compliance Information

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.4.1 Document(s) for compliance, training, awareness and screening;

1.4.2 Records of changes to access authorization lists verifying that changes were made within prescribed time frames;

1.4.3 Supporting documentation (e.g., checklists, access request/authorization documents);

1.4.4 Verification that quarterly and annual security awareness have been conducted;

1.4.5 Verification that personnel risk assessments are being conducted.

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 List 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 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 not properly documented, or

2.1.4 Training program exists, but records of training either do not exist or reveal some key personnel were not trained as required; or

2.1.5 Awareness program exists, but not applied consistently or with the minimum 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 seven calendar days or 24 hours if termination for cause; or

2.2.3 Training program exists, but doesn't not cover one of the specific items identified, 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 Access control list 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 seven business days or 24 hours if termination for cause; or

2.3.3 A personnel risk assessment program does not exist; or

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

2.4. Level 4:

2.4.1 Access control rights list does not exist; or

2.4.2 No training program exists addressing Critical Cyber Assets.

E. Regional Differences

1. None

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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1304 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–005–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–005–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of critical assets.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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 is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

Business and operational requirements for Critical Cyber Assets to communicate with other devices to provide data and services result in increased risks to these Critical Cyber Assets. In order to protect these assets, it is necessary to identify the electronic perimeter(s) within which these assets reside. When electronic perimeters are defined, different security levels may be assigned to these perimeters depending on the assets within these perimeter(s). In the case of Critical Cyber Assets, the security level assigned to these Electronic Security Perimeters is high.

This standard requires:

- The identification of the electronic (also referred to as logical) security perimeter(s) inside which Critical Cyber Assets reside, and all access points to these perimeter(s),
- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical assets within them, and
- The implementation of processes, tools and procedures to monitor electronic (logical) access to the perimeter(s) and the Critical Cyber Assets.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. Electronic Security Perimeter — The Electronic Security Perimeter is the logical border surrounding the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled. The Responsible Entity shall identify the Electronic Security Perimeter(s) surrounding its Critical Cyber Assets and all access points to the perimeter(s). Access points to the Electronic Security Perimeter(s) shall additionally include any externally connected communication end point (e.g. modems) terminating at any device within the Electronic Security Perimeter. Communication links connecting discrete electronic perimeters are not considered part of the security perimeter. However, end-points of these communication links within the security perimeter(s) are considered access points to the Electronic Security Perimeter(s). Where there are also non-Critical Cyber Assets within the defined Electronic Security Perimeter, these non-Critical Cyber Assets must comply with the requirements of this standard.

R2. Disabling unused Network Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.

R3. The Responsible Entity shall secure dial-up modem connections. Where remote activation of dial-up connectivity via SCADA-activated relays from the security or control center is technically feasible, dial-up equipment at unattended facilities shall be physically deactivated when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application.

R4. Electronic Access Controls — The Responsible Entity shall implement the organizational, technical, and procedural controls to permit or deny logical access at all electronic access points to the Electronic Security Perimeter(s) and the Critical Cyber Assets within the Electronic Security Perimeter(s).

R4.1. These Electronic Security Perimeter access controls shall implement an access control model, that denies access by default unless explicit access permissions are specified.

R4.2. Where external interactive logical access to the electronic access points into the Electronic Security Perimeter is implemented, the Responsible Entity shall implement strong procedural or technical measures to ensure authenticity of the accessing party. These strong procedural or technical measures shall include at least one of the following measures:

- Two-factor authentication
- Digital certificates
- Out-of-band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication

- One time use passwords
- In dial-up access, automatic number identification (ANI) to augment static user id and password authentication
- In dial-up access, call back to augment static user id and password authentication

R4.3. Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts.

R5. Monitoring Electronic Access Control — The Responsible Entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access to the electronic perimeter(s) and Critical Cyber Assets within the perimeter(s), 24 hours a day, 7 days a week.

R6. Documentation Review and Maintenance - The Responsible Entity shall ensure that all documentation required by this standard reflect current configurations and processes. The entity shall conduct a review of these documents at least every 90 calendar days to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes.

C. Measures

M1. Electronic Security Perimeter **—** The Responsible Entity shall maintain a document or set of documents depicting the Electronic Security Perimeter(s), all interconnected Critical Cyber Assets within the security perimeter, and all electronic access points to the security perimeter and to the interconnected environment(s). The entity shall ensure that all systems hosting Critical Cyber Assets have been identified and are within the Electronic Security Perimeter(s) documented.

M2. Disabling unused Network Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets.

M3. Dial-up Modems:

M3.1 The Responsible Entity shall maintain a documented policy for securing dial-up modem connections to Critical Cyber Assets, and a record of an annual audit of all dial-up modem connections and ports against the policy and documented configuration.

M3.2 The documentation shall verify that the Responsible Entity has taken the appropriate actions to secure dial-up access to all Critical Cyber Assets.

M4. Electronic Access Controls

M4.1 The Responsible Entity shall maintain a document or set of documents identifying the organizational, technical and procedural controls for logical (electronic) access and their implementation for each electronic access point to the Electronic Security Perimeter(s).

M4.2 For each control, the document or set of documents shall identify and describe, at a minimum,

M4.2.1 The access request and authorization process implemented for that control,

M4.2.2 The authentication methods used, and

M4.2.3 A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and ongoing supporting documentation (e.g. access request and authorization documents, review checklists) verifying that these have been implemented.

M5. Monitoring Electronic Access Control — The Responsible Entity shall maintain a document or set of documents to identify and describe:

M5.1 Organizational, technical and procedural controls, including tools and procedures, for monitoring electronic (logical) access.

M5.2 Supporting documents, including access records and logs, to verify that the tools and procedures are functioning and being used as designed.

M5.3 Processes, procedures and technical controls implemented to review access records for authorized access against access control rights, and report and alert on unauthorized access and attempts at unauthorized access to appropriate monitoring staff. Documents that record these reviews shall be identified.

M6. Documentation Review and Maintenance: — The Responsible Entity shall review the documents referenced in this standard at least annually and shall update these documents within 30 calendar days of the modification of the network or controls.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep document revisions and security incident related data (such as unauthorized access reports) for three (3) calendar years. Other audit records such as access records (e.g. access logs, firewall logs and intrusion detection logs) shall be kept for a minimum of 90 calendar days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement.

1.4. Additional Compliance Information

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard;

1.4.2 Records of electronic access to Critical Cyber Assets (e.g. access logs, intrusion detection logs)

1.4.3 Supporting documentation (e.g. checklists, access request/authorization documents)

1.4.4 Verification that necessary updates were made at least annually or within 90 calendar days of a modification

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 Document(s) exist, but have not been updated with known changes within the 90-calendar day period and/or,

2.1.2 Access to any Critical Cyber Asset was unmonitored for a period that does not exceed 24 hours.

2.2. Level 2:

2.2.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or,

2.2.2 Monitoring is in place, but a gap in the access records exists for one calendar day or more but for less than seven calendar days.

2.3. Level 3:

2.3.1 Electronic Security Perimeter: Document exists, but no verification that all critical assets are within the perimeter(s) described or,

2.3.2 Disabling Unused Network Ports/Services: Documents(s) exist, but a record of regular audits does not exist.

2.3.3 Electronic Access Controls:

2.3.3.1 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

2.3.3.2 Required documents exist, but records for some transactions are missing.

2.3.4 Electronic Access Monitoring:

2.3.4.1 Access not monitored to any Critical Cyber Asset for one week or more; or

2.3.4.2 Access records reveal access by personnel not approved on the access control list.

2.4. Level 4:

2.4.1 No document or no monitoring of access exists.

E. Regional Differences

1. None

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-006-1 (Draft 1, Std 1300, section 1305) (January 17, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1305 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–006–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–006–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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

2. Number: CIP–006–1

3. Purpose: This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

Business and operational requirements for the availability and reliability of Critical Cyber Assets dictate the need to physically secure these assets. In order to protect these assets, it is necessary to identify the Physical Security Perimeter(s) (nearest six-wall boundary) within which these Cyber Assets reside.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. Security Plan: The Responsible Entity shall document its implementation of the following requirements in its physical security plan.

R1.1. The identification of the Physical Security Perimeters(s) and the development of a defense strategy to protect the physical perimeter within which Critical Cyber Assets reside, and all access points to these perimeter(s).

R1.2. The implementation of the necessary measures to control access at all access points of these perimeter(s) and the Critical Assets within them.

R1.3. Implementation of processes, tools, and procedures to monitor physical access to the perimeter(s) and the Critical Cyber Assets.

R2. 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) following a generally accepted industry or government risk assessment procedure.

R3. Monitoring Physical Access Control: The Responsible Entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.

R4. Logging physical access: The Responsible Entity shall implement the technical and procedural mechanisms for logging physical access.

R5. Maintenance and testing: The Responsible Entity shall implement a maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.

R6. Documents for configuration, processes, tools, and procedures: The Responsible Entity shall maintain the specified documentation concerning its implementation of its Physical Security Plan.

C. Measures

M1. Documentation Review and Maintenance: The Responsible Entity shall review and update its physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods.

M2. Physical Security Perimeter: The Responsible Entity shall maintain a document or set of documents depicting the Physical Security Perimeter(s), and all access points to every such perimeter. The document shall verify that all Critical Cyber Assets are located within the Physical Security Perimeter(s).

M3. Physical Access Controls: The Responsible Entity shall implement one or more of the following physical access methods:

Card Key	A means of electronic access where the access rights of the cardholder are pre-defined in a computer database. Access rights may differ from one perimeter to another.
Special Locks	These may include locks with non-reproducible keys, magnetic locks that must open remotely or by a Man-trap.
Security Officers	Personnel responsible for controlling physical access 24 hours a day. These personnel shall reside on-site or at a central monitoring station.
Security Enclosure	A cage/safe/cabinet system that controls physical access to the Critical Cyber Asset (for environments where the nearest six-wall perimeter cannot be secured).

Other Authentication Devices	Biometric, keypad, token, or other devices that are used to control access to the Cyber Asset through personnel authentication.

In addition, the Responsible Entity shall maintain documentation identifying the access control(s) implemented for all physical access point through the Physical Security Perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and revocation process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and on-going supporting documentation.

M4. Monitoring Physical Access Control: The Responsible Entity shall implement one or more of the following monitoring methods:

CCTV	Video surveillance that captures and records images of activity in or around the secure perimeter or point of facility access.
Alarm Systems	A system that indicates 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, or motion sensors.

In addition, the Responsible Entity shall maintain documentation identifying the methods for monitoring physical access. This documentation shall identify supporting procedures to verify that the monitoring tools and procedures are functioning and being used as designed. Additionally, the documentation shall describe processes to review records for unauthorized access. The Responsible Entity shall have a process for creating unauthorized access reports.

M5. Logging Physical Access: The Responsible Entity shall implement one or more of the following logging methods. Log entries shall record sufficient information to identify each individual;

Manual Logging	A log book or sign-in sheet or other record of physical access accompanied by human observation or remote verification.
Computerized Logging	Electronic logs produced by the selected access control and monitoring method.
Video Recording	Electronic capture of video images.

In addition, the Responsible Entity shall maintain documentation identifying the methods for logging physical access. This documentation shall identify supporting procedures to verify that the logging tools and procedures are functioning and being used as designed. Physical access logs shall be retained for at least 90 days.

M6. Maintenance and testing of physical security systems: The Responsible Entity shall perform and document maintenance and testing on physical security systems annually. This documentation shall be maintained for a period of one year.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep document revisions and other security event-related data including unauthorized access reports for three calendar years. The Responsible Entity shall keep audit records for 90 days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep documents specified in this standard for three calendar years.

1.4. Additional Compliance Information

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.4.1 The Physical Security Plan

1.4.2 Document(s) for configuration, processes, tools, and procedures as described in this standard.

1.4.3 Records of physical access to Critical Cyber Assets (e.g., manual access logs, automated access logs).

1.4.4 Supporting documentation (e.g., checklists, access request/authorization documents)

1.4.5 Verification that necessary updates were made at least annually or within 90 days of a modification.

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 Document(s) exist, but have not been updated or reviewed within the last 90 days and/or

2.1.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than seven days, but less than 1 month.

2.2. Level 2:

2.2.1 Document(s) exist, but have not been updated or reviewed in the last 6 months and/or

2.2.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than one month, but less than three months.

2.3. Level 3:

2.3.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or

2.3.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than three months.

2.4. Level 4:

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

E. Regional Differences

1. None

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 15, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1306 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–007–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–007–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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 is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

While there are significant differences between attended and unattended facilities that contain Critical Cyber Assets, the requirements below will apply to both unless specifically differentiated.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. Test Procedures — Attended Facilities: The Responsible Entity shall use documented information security test procedures to augment functional test and acceptance procedures for all new systems and significant changes to existing critical cyber security assets. The Responsible Entity shall ensure that significant changes include but are not limited to security

patches, cumulative service packs, new releases, upgrades or versions to operating systems, application, database or other third party software, and firmware.

These tests are required to mitigate risk from known vulnerabilities affecting operating systems, applications, and network services. Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation.

The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities on a controlled non-production system prior to being rolled into production.

R2. Test Procedures – Unattended Facilities: The Responsible Entity shall not store test documentation, security procedures, and acceptance procedures at an unattended facility but at another secured attended facility. The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.

R3. Account and Password Management: The Responsible Entity shall establish an account password management program to provide for access authentication, auditability of user activity, and to minimize the risk to unauthorized system access by compromised account passwords. The Responsible Entity shall establish, implement, and document end user account (administrator, system, and individual) management that include but are not limited to:

R3.1. Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access controls, certificates, or bio-metric), the Responsible Entity shall use accounts that have a strong password. To the extent allowed by the existing technology, a password must consist of a combination of alpha, numeric, and special characters with a minimum of six characters. Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking.

R3.2. Generic Account Management – Attended: The Responsible Entity shall have a process for managing factory default accounts, e.g., administrator or guest. 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. Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entity shall have a policy for managing the appropriate use of group 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, e.g., change in assignment or exit.

R3.3. Generic Account Management – Unattended: For unattended facilities, the Responsible Entity shall ensure the physical access to Cyber Assets by approved users is authorized by a control or security center operator on an instance-by-instance basis.

R3.4. Access Reviews – Attended: The Responsible Entity shall ensure a designated approver reviews access to Critical Cyber Assets, e.g., computer and/or network accounts and access rights, at least semi-annually. Unauthorized, invalidated, expired, or unused computer and/or network accounts shall be disabled.

R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber-related work performed on Cyber Assets at unattended facilities.

R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges for both attended and unattended facilities. The policy shall support a compliance audit of all account usage to an individually named person, i.e., individually named user accounts, or, personal registration for any generic accounts in order to establish accountability of usage.

R4. Security Patch Management: The Responsible Entity shall establish a formal security patch management program for tracking, evaluating, testing, and installation of applicable security patches and upgrades to critical cyber security assets.

R4.1. The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based assessment, so as to avoid un-necessary and excessive patching.

R4.2. The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.

R4.3. In the case where installation of the patch is not possible, the Responsible Entity shall use and document a compensating measure(s).

R5. Integrity Software

R5.1. The Responsible Entity shall use integrity software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure, and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter.

R5.2. The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.

R5.3. In the case where integrity software is not used, e.g., operational incompatibility or not available for a particular computer platform, the Responsible Entity shall use and document a compensating measure(s).

R5.4. Where repetitious application of software updates are necessary, such as at unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware.

R6. Identification of Vulnerabilities and Responses

R6.1. The Responsible Entity shall perform a vulnerability assessment at least annually that includes:

R6.1.1. A diagnostic review of the access points to the Electronic Security Perimeter

R6.1.2. Scanning for open ports/services and modems

R6.1.3. Factory default accounts

R6.1.4. Security patch and anti-virus version levels

R6.2. The Responsible Entity shall implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment.

R6.3. For unattended facilities that contain Critical Cyber Assets, the Responsible Entity shall perform a limited vulnerability assessment prior to each upgrade as possible given the technical capability of the Cyber Assets.

R7. Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the Responsible Entity shall ensure it is possible to create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement.

R7.1. The Responsible Entity shall retain said log data for a period of ninety (90) calendar days. In the event a Cyber Security Incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) calendar years in an exportable format, for possible use in further event analysis.

R7.2. In lieu of automatically generated logs at unattended facilities, the Responsible Entity shall collect and retain the physical access and change records of users at each approved access session, or at a minimum annually.

R8. Change Control and Configuration Management

R8.1. The Responsible Entity shall establish a change control process that provides a controlled environment for modifying all hardware and software for Critical Cyber Assets. The process shall include change management procedures that at a minimum provide testing, modification of audit trails, problem identification, a back-out and recovery process should modifications fail, to ultimately ensure the overall integrity of the Critical Cyber Assets.

R8.2. The Responsible Entity shall ensure the controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility. The change control process for Cyber Assets at unattended facilities shall prevent the inadvertent dissemination of faulty or compromised software to multiple unattended sites.

R9. Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.

R10. Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets used for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified indications, as implemented.

For Critical Cyber Assets in use at unattended facilities that are not capable of being electronically monitored remotely, the Responsible Entity shall review and document pertinent metrics manually during routine access/service to said equipment.

R11. Back up and Recovery: The Responsible Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site.

C. Measures

M1. Test Procedures: For all Critical Cyber Assets, the Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion.

M2. Account and Password Management: The Responsible Entity shall maintain a documented password policy and record of semi-annual audit of this policy against all accounts on Critical Cyber Assets. The documentation shall verify that all accounts comply with the password policy and that obsolete accounts are promptly disabled. Review access permissions within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change n status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).

M3. Security Patch Management: The Responsible Entity's change control documentation shall include a record of all security patch installations including: date of testing, test results, approval for installation, compensating measures, and installation date.

M4. Integrity Software: The Responsible Entity's change control documentation shall include a record of all integrity software installations including:

M4.1 Version level actively in use

M4.2 Installation date

M4.3 Or provide documentation for other compensating measures taken

M5. Identification of Vulnerabilities and Responses:

M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities.

M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.

M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.

M6. Retention of Logs:

M6.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all log data captured from the Critical Cyber Assets.

M6.2 The documentation shall verify that the Responsible Entity is retaining information that may be vital to internal and external investigations of cyber events involving Critical Cyber Assets.

M7. Change Control and Configuration Management:

M7.1 The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets.

M7.2 The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to its Critical Cyber Assets.

M8. Disabling Unused Host Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets.

M9. Operating Status Monitoring Tools: The Responsible Entity shall maintain documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of Critical Cyber Assets.

M10. Back-up and Recovery:

M10.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all Critical Cyber Assets' information backup data and tapes.

M10.2 The documentation shall also include recovery procedures for reconstructing any Critical Cyber Asset from the backup data, and a record of the annual restoration verification exercise.

M10.3 The documentation shall verify that the Responsible Entity is capable of recovering from the failure or compromise of a Critical Cyber Asset.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three calendar years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep documents specified in this standard for three calendar years.

1.4. Additional Compliance Information

The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard.

1.4.2 System log files as described in measure M6.

1.4.3 Supporting documentation showing verification that system management policies and procedures are being followed (e.g., test records, installation records, checklists, quarterly/monthly audit logs, etc.).

2. Levels of Non-Compliance

2.1. Level 1: Document(s) exist, but does not cover up to two of the specific items identified and/or the document has not been reviewed or updated in the last 12 months.

2.2. Level 2: Document(s) exist, but does not have three of the specific items identified and/or

2.2.1 A gap in the reviews for the following items exists:

2.2.1.1 Access Reviews (semi-annually for attended facilities, periodically for unattended facilities).

2.2.1.2 Security Patch Management (monthly)

2.2.1.3 Integrity Software (monthly)

2.2.2 Retention of system logs exists, but a gap of greater than three days but less than seven days exists.

2.3. Level 3:

2.3.1 Document(s) exist, but more than three of the items specified are not covered.

2.3.2 Test Procedures: Document(s) exist, but documentation verifying that changes to Critical Cyber Assets tested is incomplete or changes to Critical Cyber Assets were not tested.

2.3.3 Account and Password Management: Document(s) exist, but documentation verifying accounts and passwords comply with the policy does not exist.

2.3.4 Security Patch Management: Document exists, but records of security patch installations are incomplete.

2.3.5 Integrity Software: Documentation exists, but verification that all Critical Cyber Assets are being kept up to date on anti-virus software or that compensating measures are being taken does not exist.

2.3.6 Identification of Vulnerabilities and Responses:

2.3.6.1 Document exists, but annual vulnerability assessment was not completed and/or

2.3.6.2 Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist.

2.3.7 Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists.

2.3.8 Disabling Unused Host Ports/Services: Documents(s) exist, but a record of regular audits does not exist.

2.3.9 Change Control and Configuration Management: N/A

2.3.10 Operating Status Monitoring Tools: N/A

2.3.11 Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist.

2.4. Level 4: No documentation exists.

E. Regional Differences

1. None

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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1307 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–008–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–008–1	September 1, 2005
8. Effective date	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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 Response Planning

2. Number: CIP–008–1

3. Purpose: This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

Security measures designed to protect Critical Cyber Assets from intrusion, disruption, or other forms of compromise must be monitored on a continuous basis. This standard requires responsible entities to define the procedures that must be followed when Cyber Security Incidents are identified. This standard requires:

- Developing and maintaining documented procedures,
- Classification of incidents,
- Actions to be taken, and
- Reporting of Incidents.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting, and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:

R2. Incident Classification: The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents.

R3. Cyber Security Incident Response Actions: The Responsible Entity shall define incident response actions, including roles and responsibilities of incident response teams, incident handling procedures, escalation, and communication plans.

R4. Cyber Security Incident Reporting: The Responsible Entity shall report all Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC) in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary.

C. Measures

M1. The Responsible Entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and Cyber Security Incident reporting requirements at least annually or within 90 calendar days of known changes.

M2. The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep documents specified in this standard for three calendar years.

1.4. Additional Compliance Information

The Responsible Entity shall keep all records related to Cyber Security Incidents for three calendar years. This includes, but is not limited to the following:

1.4.1 System and application log file entries,

1.4.2 Video, and/or physical access records,

1.4.3 Documented records of investigations and analysis performed,

1.4.4 Records of any action taken including any recovery actions initiated.

1.4.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1 Documentation exists, but has not been updated with known changes within 90 calendar days.

2.2. Level 2:

2.2.1 Incident response documentation exists, but has not been updated or reviewed in the last 12 months and/or

2.2.2 Records related to Cyber Security Incidents are not maintained for three years or are incomplete.

2.3. Level 3:

2.3.1 Incident response documentation exists but is incomplete and/or

2.3.2 Cyber Security Incidents have occurred but were not reported to the ES ISAC

2.4. Level 4: No documentation exists.

E. Regional Differences

1. None

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)

Description of Current Draft:

The current draft reformats Standard 1300, section 1308 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–009–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–009–1	September 1, 2005
8. Effective date.	October 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 Asset: 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 electric grid, or would cause significant risk to public health and safety.

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

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

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

- Compromises, or was an attempt to compromise, the electronic 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 the network or group of sub-networks (the "secure network") to which the Critical Cyber Assets are connected, and for which access is controlled.

Physical Security Perimeter: The physical 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

2. Number: CIP–009–1

3. Purpose: This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

4. Applicability

When used within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator

4.2. Balancing Authority

4.3. Interchange Authority

4.4. Transmission Service Provider

4.5. Transmission Owner

4.6. Transmission Operator

4.7. Generator Owner

4.8. Generator Operator

4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1.

5. (Proposed) Effective Date: October 1, 2005

B. Requirements

R1. The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan(s) at least annually.

R2. The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.

R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.

R4. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Asset within seven (7) calendar days of development or modification.

R5. The Responsible Entity shall develop training and awareness for its recovery plan(s) that follow the requirements set forth in Standard CIP–004–1 — Personnel and Training.

C. Measures

M1. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years.

M2. The Responsible Entity shall review and update if needed, its response to events of varying duration and severity annually or as necessary.

M3. The Responsible Entity shall review and update recovery plan(s) annually.

M4. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe

The Responsible Entity shall make the documents described in this standard available for inspection by the compliance monitor upon request. The performance-reset period shall be one (1) calendar year.

1.3. Data Retention

The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

2.1. Level 1: Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year.

2.2. Level 2: Recovery plan(s) have not been reviewed, exercised, or training performed.

2.3. Level 3: Recovery plan(s) address neither the types of events that are necessary nor any specific roles and responsibilities.

2.4. Level 4: No recovery plan(s) exist.

E. Regional Differences

1. None

Version History

Version	Date	Action	Change Tracking