Special Procedures

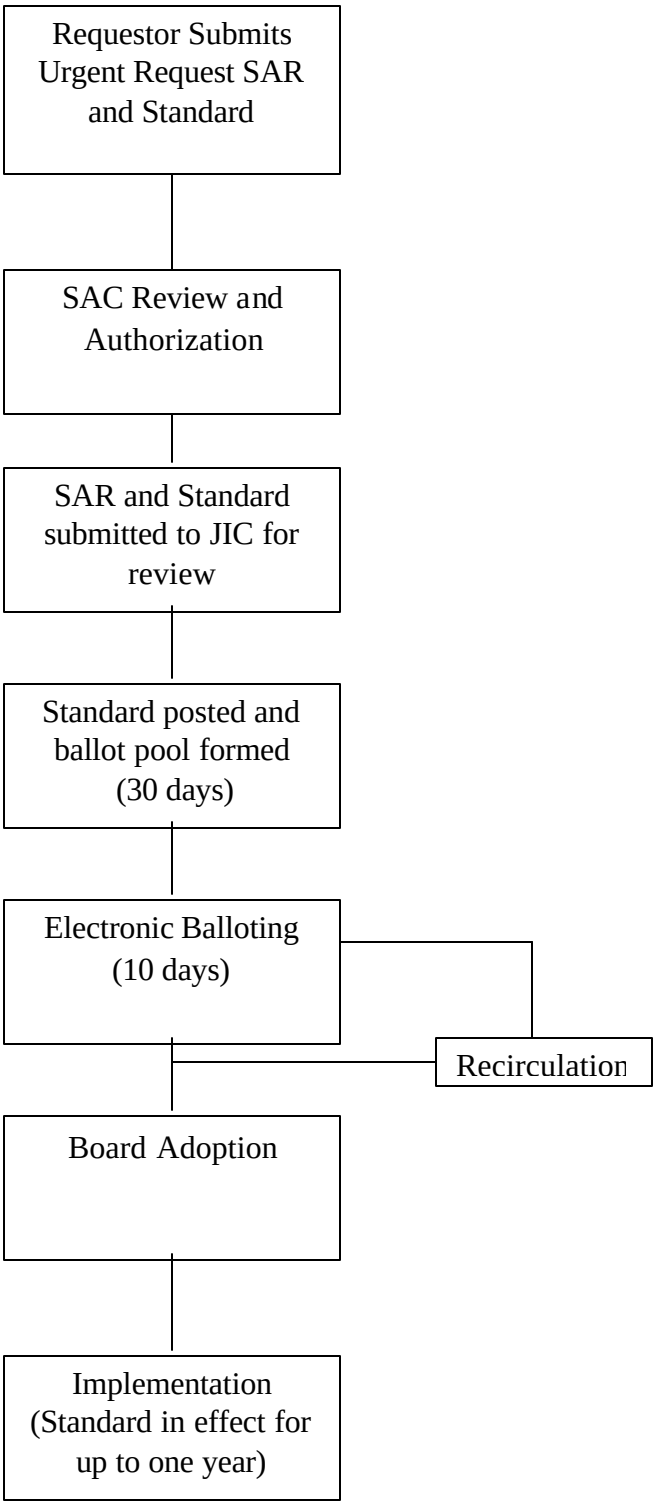
Urgent Actions

Under certain conditions, the Standards Authorization Committee may designate a proposed standard or revision to a standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact reliability of the bulk electric systems. **The Standards Authorization Committee must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or impleme nt a standard.**

A Requester prepares a SAR and a draft of the proposed standard and submits it to the Standards Process Manager. The SAR must include a justification for urgent action. The Standards Process Manager submits the request to the Standards Authorization Committee for its consideration. If the Standards Authorization Committee designates the requested standard or revision as an urgent action item, then the Standards Process Manager shall immediately seek participants for a ballot pool from the registered ballot body and shall post the draft for a minimum of 30 days. At the conclusion of the posting period, a ten-day electronic ballot is conducted, following the same voting procedure as a traditional NERC reliability standard.

Any standard approved as an urgent action shall have a termination date specified that shall not exceed one year from the approval date. Should there be a need to make the standard permanent, then the standard would be required to go through the full consensus process. Urgent actions that expire may be renewed no more than once using the urgent action process again, in the event a permanent standard is not adopted.

Urgent Request Flow Diagram



Standard Authorization Request Form URGENT ACTION

Title of Proposed Standard	Cyber Security
Request Date	April 2, 2003

SAR Requestor Information

Name	Charles Noble (on behalf of CIPAG)	**SAR Type** (Check box for one of these selections.)	
Company		☒	New Standard
Telephone		☐	Revision to Existing Standard
Fax		☐	Withdrawal of Existing Standard [1]
E-mail		☒	Urgent Action

Purpose/Industry Need (Provide one or two sentences.)

To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems.

Note: Due to the increasing threats to electric system reliability stemming from cyber attacks, this request is being submitted as an **Urgent Action Request.** Please see the detailed description for the justification for this request.

Brief Description

This standard will require that critical cyber assets related to the reliable operation of the bulk electric systems are identified and protected. Requirements will be included in the standard to identify the responsible person(s), create and implement programs and procedures, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
☒	Interchange Authority	Authorizes valid and balanced Interchange Schedules
☐	Planning Authority	Plans the bulk electric system
☒	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
☐	Transmission Owner	Owns transmission facilities
☒	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
☐	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer
☒	Generator	Owns and operates generation unit(s) or runs a market for generation products that performs the functions of supplying energy and Interconnected Operations Services
☐	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required
☒	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk electric systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk electric systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk electric systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk electric systems.
☒	6. Personnel responsible for planning and operating interconnected bulk electric systems shall be trained, qualified and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk electric systems shall be assessed, monitored and maintained on a wide area basis.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. The planning and operation of bulk electric systems shall recognize that reliability is an essential requirement of a robust North American economy. Yes
2. An Organization Standard shall not give any market participant an unfair competitive advantage. Yes
3. An Organization Standard shall neither mandate nor prohibit any specific market structure. Yes
4. An Organization Standard shall not preclude market solutions to achieving compliance with that Standard. Yes
5. An Organization Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Detailed Description

Justification for Urgent Action

1. There have already been incidents that impacted cyber systems that are critical to electric system reliability.

2. The frequency and severity of cyber attacks are increasing.

3. World events may lead to cyber attacks that impact bulk electric system reliability.

4. The standard is based upon guidelines established by the NERC Critical Infrastructure Protection Advisory Group (CIPAG) and approved by the NERC Board of Trustees. These guidelines were submitted to the industry for review and comment. Comments received were reviewed and included in the guidelines, as appropriate.

5. The standard is also based upon the proposed cyber security standard drafted by a NERC-sponsored industry group, approved by CIPAG and the NERC Board of Trustees, and submitted to FERC at its request. Two industry comment periods were included in the development of this proposed cyber security standard.

6. It is unclear when FERC will establish cyber security requirements; these requirements are needed as soon as possible to maintain the reliability of the electric systems.

Reliable electric system operations are highly interdependent, and a failure of one part of the generation, transmission or grid management system can compromise the reliable operation of a major portion of the regional grid. Similarly, the wholesale electric market as a network of economic transactions and interdependencies relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch and market software and systems. Because of this mutual vulnerability and interdependence, it is necessary to safeguard the critical cyber assets that support bulk electric system operations by establishing standards to assure that a lack of cyber security for one critical asset does not compromise security and risk grid or market failure.

This standard requires that responsible entities understand the role of cyber security in electric infrastructure reliability, have identified their critical cyber assets related to bulk electric system operations, and have a security program in place. This program should mitigate the impact to bulk electric system operations from acts, either accidental or malicious, that could cause wide-ranging, harmful impacts. A basic cyber security program for bulk electric system operations shall cover governance, planning, prevention, operations, incident response, and business continuity. This standard is intended to ensure that appropriate mitigating plans and actions are in place, recognizing the differing roles of each responsible entity and the differing risks being managed.

This cyber security standard shall primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel. In addition, physical security shall be addressed to the extent that it is necessary to assure a secure physical environment for cyber resources.

This standard will apply to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Operator, Generator, and Load Serving Entity and functions.

This standard provides definition of terms and the minimum requirements to implement and maintain a cyber security program to protect cyber assets critical to reliable electric system operations.

Definitions

Critical Cyber Assets: Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Electronic Security Perimeter: The border surrounding the network or group of sub-networks (the "secure network") to which the critical cyber assets are connected.

Physical Security Perimeter: The border surrounding computer rooms, telecommunications rooms, operations centers, and other clearly defined locations in which critical cyber assets are housed and access is controlled.

Cyber Security Incident: Any event or failure (malicious or otherwise) that disrupts the proper operation of a Critical Cyber Asset.

Incident Response: Responding to, and reporting a cyber security incident.

Compliance Monitor: The organization responsible for monitoring compliance with this standard in accordance with the NERC compliance enforcement program.

Related SARs

SAR ID	Explanation
None	

Regional Differences

Region	Explanation
None	

Related NERC Planning Standards/Operating Policies

Standard No.	Explanation
None	

Industry Representatives who participated in developing this SAR	Charles Noble – ISO New England Jerry Freese – American Electric Power Larry Brown – Edison Electric Institute Ken Hall – Edison Electric Institute Larry Bugh – ECAR Regional Council Scott Mix – Electric Power Research Institute Jim Orcheson – Independent Market Operator (Ontario) Roger Lampila – New York ISO James Strange –American Public Power Association

These definitions will be posted and balloted along with the cyber security standards, but will not be restated in the cyber security standards. Instead, they will be included in a separate "Definitions" section containing definitions relevant to all standards that NERC develops.

DEFINITIONS

Critical Cyber Assets: Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Electronic Security Perimeter: The border surrounding the network or group of sub-networks (the "secure network") to which the critical cyber assets are connected.

Physical Security Perimeter: The border surrounding computer rooms, telecommunications rooms, operations centers, and other clearly defined locations in which critical cyber assets are housed and access is controlled.

Cyber Security Incident: Any event or failure (malicious or otherwise) that disrupts the proper operation of a critical cyber asset.

Incident Response: Responding to, and reporting a cyber security incident.

Compliance Monitor: The organization responsible for monitoring compliance with this standard in accordance with the NERC compliance enforcement program.

1200 ¾ CYBER SECURITY

1200 Cyber Security Policy

1201 Critical Cyber Assets

1202 Electronic Security Perimeter

1203 Electronic Access Controls

1204 Physical Security Perimeter

1205 Physical Access Controls

1206 Personnel

1207 Monitoring Physical Access

1208 Monitoring Electronic Access

1209 Information Protection

1210 Training

1211 Systems Management

1212 Test Procedures

1213 Electronic Incident Response Actions

1214 Physical Incident Response Actions

1215 Recovery Plans

(a) **Purpose**: To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.

(b) **Effective Period**: This urgent request standard will be in effect for one year from the date of NERC Board of Trustees adoption or until it is replaced by a permanent standard, whichever occurs first.

(c) **Applicability:** These cyber security standards apply to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June 2001. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions.

1201 ¾ Cyber Security Policy

(a) Requirement

(1) The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create and maintain a cyber security policy for the implementation of this standard.

(2) The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity's cyber security program. This person must authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption must be documented.

(b) Measures

(1) The responsible entity shall maintain its written cyber security policy stating the entity's commitment to protect critical cyber assets.

(2) The responsible entity shall review the cyber security policy at least annually.

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

(4) The responsible entity shall maintain documentation justifying any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Written cyber security policy;

(B) The name, title, address, and phone number of the current designated senior management official and the date of his or her designation; and

(C) Documentation of justification for any deviations or exemptions.

(e) Levels of Noncompliance

(1) Level one:

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

(B) A written cyber security policy exists but has not been reviewed in the last calendar year.

(2) Level two: A current senior management official was not designated for 30 or more days, but less than 60 days during a calendar year.

(3) Level three: A current senior management official was not designated for 60 or more days, but less than 90 days during a calendar year

(4) Level four:

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

(B) No cyber security policy exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1202 ¾ Critical Cyber Assets

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its critical cyber assets.

(b) Measures

(1) The responsible entity shall maintain a document identifying critical cyber assets.

(2) The responsible entity shall review and update its critical cyber asset identification document at least annually or within 90 days of the addition or removal of any critical cyber assets.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) List of critical cyber assets; and

(B) Verification that necessary updates were made at least annually or within 90 days of the addition or removal of critical cyber assets.

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: (None specified.)

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1203 ¾ Electronic Security Perimeter

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its electronic security perimeter(s).

(b) Measures

(1) The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s). The document shall verify that all critical cyber assets are within the electronic security perimeter(s).

(2) The responsible entity shall review and update its document referenced in 1203(b)(1) at least annually or within 90 days of the modification of the network.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1203(b)(1); and

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

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: Document exists, but no verification that all critical assets are within the perimeter(s) described.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1204 ¾ Electronic Access Controls

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter.

(b) Measures

(1) The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).

(2) The responsible entity shall review and update the documentation referenced in 1204(b)(1) at least annually or within 90 days of the modification of the electronic security perimeter or the electronic access controls.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1204(b)(1); and

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

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: Document exists, but the document does not identify the electronic access controls for one or more access points.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1205 ¾ Physical Security Perimeter

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its physical security perimeter(s) for the protection of critical cyber assets.

(b) Measures

(1) The responsible entity shall maintain a document depicting the physical security perimeter(s) and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeter(s).

(2) The responsible entity shall review and update the document referenced in 1205(b)(1) at least annually or within 90 days of the modification of the network.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1205(b)(1); and

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

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: Document exists, but no verification that all critical cyber assets are within the perimeter(s) described.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1206 ¾ Physical Access Controls

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify and implement physical access controls for access to critical cyber assets within the physical security perimeter(s).

(b) Measures

(1) The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).

(2) The responsible entity shall review and update the documentation referenced in 1206(b)(1) at least annually or within 90 days of the modification of the physical security perimeter(s) or the physical access controls.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1206(b)(1); and

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

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: Document exists, but the document does not identify the physical access controls for one or more access points.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1207 ¾ Personnel

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets.

(b) Measures

(1) The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s).

(2) The responsible entity shall review the document referred to in 1207(b)(1) at least quarterly and update the document within 24 hours of any change.

(3) The responsible entity shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1207(b)(1);

(B) Verification that necessary updates were made at least quarterly or within 24 hours of a modification; and

(C) Verification that personnel background checks are being conducted consistent with access granted to them.

(e) Levels of Noncompliance

(1) Level one:

(A) 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

(B) One instance of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours.

(2) Level two:

(A) Access control rights list is available, but has not been updated or reviewed for more than 6 months but less than 12 months; or

(B) More than one but not more than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours.

(3) Level three:

(A) Access control rights list is available, but does not include service vendors;

(B) More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours; or

(C) No personnel background screening conducted.

(4) Level four: Access control rights list does not exist.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1208 ¾ Monitoring Physical Access

(a) Requirements

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor physical access to critical cyber assets 24 hours a day, 7 days a week.

(b) Measures

(1) The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are functioning and being used as planned.

(2) The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for six months. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1208(b)(1);

(B) Records of physical access to critical cyber assets; and

(C) Demonstration that the list of access control rights is controlled by video or other physical monitoring.

(e) Levels of Noncompliance

(1) Level one: Monitoring is in place, but a gap in the logs or other measures exists for less than seven days.

(2) Level two: Access not monitored to any critical cyber asset for less than one day.

(3) Level three:

(A) Access not monitored to any critical cyber asset for more than one day but less than one week; or

(B) Log or other monitoring reveals access by personnel not approved on the access control list.

(4) Level four: No monitoring of access exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1209 ¾ Monitoring Electronic Access

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week.

(b) Measures

(1) The responsible entity shall maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned.

(2) The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for six months. The compliance monitor shall keep audit records data for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1209(b)(1);

(B) Records of electronic access to critical cyber assets; and

(C) Demonstration that the list of access control rights is verified.

(e) Levels of Noncompliance

(1) Level one: Monitoring is in place, but a gap in the access records exists for less than seven days.

(2) Level two: Access not monitored to any critical cyber asset for less than one day.

(3) Level three:

(A) Access not monitored to any critical cyber asset for more than one day but less than one week; or

(B) Access records reveal access by personnel not approved on the access control list.

(4) Level four: No monitoring of access exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1210 ¾ Information Protection

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall protect information associated with critical cyber assets and the policies and practices used to keep them secure.

(b) Measures

(1) The responsible entity shall maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At a minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations.

(2) The responsible entity shall review and update the document referred to in 1210(b)(1) as necessary and at least annually.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the document as described in 1210(b)(1) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Document exists, but document has not been reviewed or updated in the last 12 months.

(2) Level two: Document exists, but does not cover one of the specific items identified.

(3) Level three: Document exists, but does not cover three of the specific items identified.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1211 ¾ Training

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall train personnel commensurate with their access to critical cyber assets. The training shall address, at a minimum: the cyber security policy, physical and electronic access controls to critical cyber assets, the release of critical cyber asset information, potential threat incident reporting, and action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Training shall be conducted upon initial employment and reviewed annually.

(b) Measures

(1) The responsible entity shall develop and maintain a company-specific cyber security training program that includes, at a minimum, the following required items:

(A) The cyber security policy;

(B) Physical and electronic access controls to critical cyber assets;

(C) The release of critical cyber asset information;

(D) Potential threat incident reporting; and

(E) Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.

(2) The responsible entity shall maintain a document identifying all personnel who have access to critical cyber assets and the date of the successful completion of their training.

(3) The responsible entity shall document that it has reviewed its training program at least annually.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the training documents described in 1211(b)(1), (2), and (3) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Training program exists, but records of training either do not exist or reveal some key personnel not trained as required.

(2) Level two: Training program exists, but does not cover one of the specific items identified.

(3) Level three: Document exists, but does not cover two of the specific items identified.

(4) Level four: No training program exists addressing critical cyber assets.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1212 ¾ Systems Management

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address:

(1) The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment;

(2) The authorization and periodic review of computer accounts and access rights;

(3) The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights;

(4) The disabling of unused network services and ports;

(5) Secure dial-up modem connections;

(6) Firewall management;

(7) Intrusion detection processes;

(8) Security patch management;

(9) The installation and update of anti-virus software;

(10) The retention and review of operator logs, application logs, and intrusion detection logs; and

(11) Identification of vulnerabilities and responses.

(b) Measures

(1) The responsible entity shall maintain a document identifying system management policies and procedures.

(2) The responsible entity shall review and update the document referred to in 1212(b)(1) as necessary and at least annually.

(3) The system management policies and procedures document shall address all items in requirement 1212(a).

(4) The responsible entity shall implement system management policies and procedures as described in the system management policies and procedures document.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1212(b)(1); and

(B) Verification that system management policies and procedures are being followed.

(e) Levels of Noncompliance

(1) Level one:

(A) Document exists, but does not cover one of the specific items identified; or

(B) The document has not been reviewed or updated in the last 12 months.

(2) Level two: Document exists, but does not cover three of the specific items identified.

(3) Level three: Document exists, but does not cover five of the specific items identified.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1213 ¾ Test Procedures

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment.

(b) Measures

(1) The responsible entity shall maintain a document identifying test and acceptance criteria for the installation or modification of critical cyber assets.

(2) The responsible entity shall maintain a document verifying that it has implemented the test and acceptance criteria.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the documents described in 1213(b)(1) and (2) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Test procedures and acceptance criteria document exists, but has not been reviewed or updated within the last 12 months.

(2) Level two: (None specified.)

(3) Level three: (None specified.)

(4) Level four: Test procedures and acceptance criteria document does not exist.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1214 ¾ Electronic Incident Response Actions

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.

(b) Measures

(1) The responsible entity shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.

(2) The document in 1214(b)(1) shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the document described in 1214(b)(1) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Electronic incident response plan exists, but has not been reviewed or updated in the last 12 months.

(2) Level two: (None specified.)

(3) Level three:

(A) Document exists, but does not assign responsibilities; or

(B) Document exists, but does not require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure.*

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed this urgent action standard.

1215 ¾ Physical Incident Response Actions

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define physical incident response actions, including roles and responsibilities assigned by individual or job function.

(b) Measures

(1) The responsible entity shall maintain a document defining the physical incident response action, including actions, roles and responsibilities.

(2) The document in 1215(b)(1) shall require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the document described in 1215(b)(1) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Physical incident response plan exists, but has not been reviewed or updated in the last 12 months.

(2) Level two: (None specified.)

(3) Level three:

(A) Document exists, but does not assign responsibilities; or

(B) Document exists, but does not require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure.*

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1216 ¾ Recovery Plans

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Each responsible entity shall exercise these plans at least annually. The plans and procedures shall define roles and responsibilities by individual or job function.

(b) Measures

(1) The responsible entity shall maintain a document defining the action plan and procedures used to recover or re-establish critical cyber assets following a cyber security event, including actions, roles and responsibilities.

(2) The responsible entity shall maintain a document verifying that the action plan is exercised via drill at least annually.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the documents described in 1217(b)(1) and (2) available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Action plans and procedures exist, but have not been reviewed or updated in the last 12 months.

(2) Level two: Action plans and procedures have not been exercised through a drill in the last 12 months.

(3) Level three: Action plans and procedures do not define specific roles and responsibilities.

(4) Level four: No action plans of procedures exist.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

Sanctions Table

The following is an approved matrix of compliance sanctions developed by the Compliance Subcommittee as part of the NERC Compliance Enforcement Program and was approved by the NERC Board of Trustees.

Levels of noncompliance are tied to this matrix. The matrix is divided into four levels of increasing noncompliance vertically and the number of violations in a defined period at a given level horizontally.

In the enforcement matrix, note that there are three sanctions that can be used: a letter, a fixed fine, and a $$ per MW fine.

Letter

The letter is a sanction used to notify company executives, Regional officers, and regulators when an entity is non-compliant. The distribution of the letter varies depending on the severity of the noncompliance. It is used first to bring noncompliance to light to people who can influence the operation to become compliant.

- Letter (A) — Letter to the entity's vice president level or equivalent informing the entity of noncompliance, with copies to the data reporting contact, and the entity's highest ranking Regional Council representative.
- Letter (B) — Letter to the entity's chief executive officer or equivalent, with copies to the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which noncompliance occurred.
- Letter (C) — Letter to the entity's chief executive officer and chairman of the board, with copies to the NERC president, regulatory authorities having jurisdiction over the non-compliant entity (if requested by such regulatory authorities), the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which non-compliance occurred.

Fixed Dollars

This sanction is used when a letter is not enough and a stronger message is desired. Fixed dollars are typically assigned as a one-time fine that is ideal for measures involving planning-related standards. Many planning actions use forward-looking assumptions. If those assumptions prove wrong in the future, yet they are made in good faith using good practices, entities should not be harshly penalized for the outcome.

Dollars per MW

Dollars per MW sanctions are oriented toward operationally based standards. The MW can be load, generation, or flow on a line. Reasonableness of a sanction needs to be figured into assessing $/MW penalties. Assessing large financial penalties is not the goal, but sending a message with proper emphasis on $$$ can be controlled with the multiplier.

Occurrence Period Category	Number of Violations in Occurrence Period at a Given Level			
1st Period of Violations (Fully Compliant Last Period)	1	2	3	4 or more
2nd Consecutive Period of Violations		1	2	3 or more
		$ Sanction from Table; Letter (C) only if Letter (B) previously sent		
3rd Consecutive Period of Violations			1	2 or more
			$ Sanction from Table; Letter (C) only if Letter (B) previously sent	
4th or greater Consecutive Period of Violations				1
				$ Sanction from Table; Letter (C)

Level of Non-Compliance	Sanctions Associated with Non-compliance			
Level 1	Letter (A)	Letter (A)	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW
Level 2	Letter (A)	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW
Level 3	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW	Letter (B) and $6,000 or $6 Per MW
Level 4	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW	Letter (B) and $6,000 or $6 Per MW	Letter (B) and $10,000 or $10 Per MW

Interpreting the Tables:

- These tables address penalties for violations of the same measure occurring in consecutive compliance reporting periods.
- If a participant has non-compliant performance in consecutive compliance reporting periods, the sanctions applied are more punitive.