These definitions will be posted and balloted along with the standard, but will not be restated in the standard. Instead, they will be included in a separate glossary of terms relevant to all standards that NERC develops.

DEFINITIONS

Cyber Assets: Those systems (including hardware, software, and data) and communication networks (including hardware, software, and data) associated with bulk electric system assets.

Critical Cyber Assets: Those cyber assets that perform critical bulk electric system functions such as telemetry, monitoring and control, automatic generator control, load shedding, black start, real-time power system modeling, special protection systems, power plant control, substation automation control, and real-time inter-utility data exchange are included at a minimum. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets.

Bulk Electric System Asset: Any facility or combination of facilities that, if unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, or would have a detrimental impact to the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

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.

Responsible Entity: The organization performing the reliability function, as identified in the Reliability Function table of the Standard Authorization Request for this standard.

Incident: Any physical or cyber event that:

- disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or
- compromises, or was an attempt to compromise, the electronic or physical security perimeters.

Security Incident: Any malicious or suspicious activities which are known to cause, or could have resulted in, an incident.

1300 – Cyber Security

1301 Security Management Controls

1302 Critical Cyber Assets

1303 Personnel & Training

1304 Electronic Security

1305 Physical Security

1306 Systems Security Management

1307 Incident Response Planning

1308 Recovery Plans

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

Effective Period: This standard will be in effect from the date of the NERC Board of Trustees adoption.

Applicability: This cyber security standard applies to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity.

In this standard, the terms *Balancing Authority*, *Interchange Authority*, *Reliability Authority*, *Purchasing/Selling Entity*, and *Transmission Service Provider* refer to the entities performing these functions as defined in the Functional Model.

1301 Security Management Controls

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.

(a) Requirements

(1) Cyber Security Policy

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 policy.

(2) Information Protection

The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets.

(i) Identification

The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information.

(ii) Classification

The responsible entity shall classify information related to critical cyber assets to aid personnel with access to this information in determining what information can be disclosed to unauthenticated personnel, as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization.

(iii) Protection

Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.

(3) Roles and Responsibilities

The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation of the cyber security standard. This person 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 classified in section 1.2.

(4) Governance

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.

(5) Access Authorization

(i) The responsible entity shall institute and document a process for access management to information pertaining to or used by critical cyber assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.

(ii) Authorizing Access

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.

(iii) Access Review

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.

(iv) Access Revocation/Changes

Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented.

(6) Authorization to Place Into Production

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 as stated in 1304 and 1306 of this standard prior to the system being promoted to operate in a production environment.

(b) Measures

(1) Cyber Security Policy

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

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

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

(iv) 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.

(2) Information Protection

(i) The responsible entity shall review the information security protection program at least annually.

(ii) The responsible entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually.

(iii) The responsible entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the classification level assigned to that information.

(iv) The responsible entity shall assess the critical cyber information identification and classification procedures to ensure compliance with the documented processes at least annually.

(3) Roles and Responsibilities

(i) The responsible entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information.

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

(iii) Changes must be documented within 30 days of the effective date.

(iv) The responsible entity shall review the roles and responsibilities of critical cyber asset owners, custodians, and users at least annually.

(4) Governance

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.

(5) Access Authorization

(i) The responsible entity shall update the list of designated personnel responsible to authorize access to critical cyber information within five days of any change in status that affects the designated personnel's ability to authorize access to those critical cyber assets.

(ii) The list of designated personnel responsible to authorize access to critical cyber information shall be reviewed, at a minimum of once per quarter, for compliance with this standard.

(iii) The list of designated personnel responsible to authorize access to critical cyber information shall identify each designated person by name, title, phone, address, date of designation, and list of systems/applications they are responsible to authorize access for.

(iv) 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.

(v) The responsible entity shall review user access rights every quarter to confirm access is still required.

(6) Authorization to Place Into Production

Responsible entities shall identify the designated approving authority responsible for authorizing systems suitable for the production environment by name, title, phone, address, and date of designation. This information will be reviewed for accuracy at least annually.

Changes to the designated approving authority shall be documented within 48 hours of the effective change.

(c) Regional Differences

None specified.

(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:

(i) Written cyber security policy;

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

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

(iv) Audit results and mitigation strategies for the information security protection program. Audit results will be kept for a minimum of three years.

(v) The list of approving authorities for critical cyber information assets.

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

(e) Levels of Noncompliance

(1) Level One

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

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

(iii) Deviations to policy are not documented within 30 days of the deviation, or

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

(v) An information security protection program exists but has not been assessed in the last calendar year, or

(vi) Processes to protect information pertaining to or used by critical cyber assets has not been reviewed in the last calendar year.

(2) Level Two

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

(ii) Access to critical cyber information is not assessed in the last 90 days, or

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

(iv) The list of designated personnel responsible to authorize access to critical cyber information has not been reviewed within 30 days of a change in designated personnel's status.

(3) Level Three

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

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

(iii) Roles and responsibilities are not clearly defined, or

(iv) Processes to authorize placing systems into production are not documented or the designated approving authority is not identified by name, title, phone, address, and date of designation.

(4) Level Four

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

(ii) No cyber security policy exists, or

(iii) No information security program exists, or

(iv) Roles and responsibilities have not been defined, or

(v) Executive management has not been engaged in the cyber security program, or

(vi) No corporate governance program exists, or

(vii) Access authorizations have not been reviewed within the last calendar year, or

(viii) There is no authorizing authority to validate systems that are to be promoted to production, or

(ix) The list of designated personnel responsible to authorize access to logical or physical critical cyber assets does not exist.

(x) Access revocations/changes are not authorized and/or documented, or

(xi) Access revocations/changes are not accomplished within 24 hours of any change in user access status.

(f) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1302 Critical Cyber Assets

Business and operational demands for maintaining and managing 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 entities identify and protect critical cyber assets related to the reliable operation of the bulk electric system.

(a) Requirements

Responsible entities shall identify their critical bulk electric system assets using their preferred risk-based assessment. An inventory of critical bulk electric system assets is then the basis to identify a list of associated critical cyber assets that is to be protected by this standard.

(1) Critical Bulk Electric System Assets

The responsible entity shall identify its critical bulk electric system assets. A critical bulk electric system asset consists of 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. Those critical bulk electric system assets include assets performing the following:

(i) Control centers performing the functions of a Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities.

A) Bulk electric system tasks such as telemetry, monitoring and control, automatic generator control, real-time power system modeling, and real-time inter-utility data exchange.

(ii) Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL)

(iii) Generation:

A) Generating resources under control of a common system that meet criteria for a Reportable Disturbance (NERC Policy 1.B, Section 2.4)

B) Generation control centers that have control of generating resources that when summed meet the criteria for a Reportable Disturbance (NERC Policy 1.B, Section 2.4).

(iv) System Restoration:

A) Black start generators.

B) Substations associated with transmission lines used for initial system restoration.

(v) Automatic load shedding under control of a common system capable of load shedding 300 MW or greater.

(vi) Special Protection Systems whose misoperation can negatively affect elements associated with an IROL.

(vii) Additional Critical Bulk Electric System Assets

A) The responsible entity shall utilize a risk-based assessment to identify any additional critical bulk electric system assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure.

(2) Critical Cyber Assets

(i) The responsible entity shall identify cyber assets to be critical using the following criteria:

A) The cyber asset supports a critical bulk electric system asset, and

B) the cyber asset uses a routable protocol, or

C) the cyber asset is dial-up accessible.

D) Dial-up accessible critical cyber assets, which do use a routable protocol require only an electronic security perimeter for the remote electronic access without the associated physical security perimeter.

E) Any other cyber asset within the same electronic security perimeter as the identified critical cyber assets must be protected to ensure the security of the critical cyber assets as identified in 1302.1.2.1.

(3) A senior management officer must approve the list of critical bulk electric system assets and the list of critical cyber assets.

(g) Measures

(1) Critical Bulk Electric System Assets

(i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1.

(2) Risk-Based Assessment

(i) The responsible entity shall maintain documentation depicting the risk-based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.

(3) Critical Cyber Assets

(i) The responsible entity shall maintain documentation listing all cyber assets as identified under 1302.1.2

(4) Documentation Review and Maintenance

(i) The responsible entity shall review, and as necessary, update the documentation referenced in 1302.2.1, 1302.2.2 and 1302.2.3 at least annually, or within 30 days of the addition or removal of any critical cyber assets.

(5) Critical Bulk Electric System Asset and Critical Cyber Asset List Approval

(i) A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained.

(ii) A properly dated record of the senior management officer's approval of the list of critical cyber assets must be maintained.

(h) Regional Differences

None specified.

(i) 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) Verify annually that necessary updates were made within 30 days of asset additions, deletions or modifications. 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:

(i) Documentation of the approved list of critical bulk electric system assets,

(ii) Documentation depicting the risk-based assessment methodology used to identify its critical bulk electric system assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure,

(iii) Documentation of the approved list of critical cyber assets, and

(iv) Documentation of the senior management official's approval of both the critical bulk electric and cyber security assets lists.

(j) Levels of Noncompliance

(1) Level One

The required documents exist, but have not been updated with known changes within the 30-day period.

(2) Level Two

The required documents exist, but have not been approved, updated, or reviewed in the last 12 months.

(3) Level Three

One or more document(s) missing.

(4) Level Four

No document(s) exist.

(k) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1303 Personnel & Training

Personnel having 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.

(a) Requirements

(1) Responsible entity shall comply with the following requirements of this standard: Awareness: Security awareness programs shall be developed, maintained and documented to ensure personnel subject to the standard receive on-going reinforcement in sound security practices.

(2) Training: All personnel having 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.

(3) Records: Records shall be prepared and maintained to document training, awareness reinforcement, and background screening of all personnel having access to critical cyber assets and shall be provided for authorized inspection upon request.

(4) Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets.

(l) Measures

(1) 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:

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

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

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

(2) Training

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

(i) The cyber security policy;

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

(iii) The proper release of critical cyber asset information;

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

(3) Records

This responsible entity shall develop and maintain records to adequately document compliance with section 1303.

(i) The responsible entity shall maintain documentation of all personnel who have access to critical cyber assets and the date of completion of their training.

(ii) The responsible entity shall maintain documentation that it has reviewed its training program annually.

(4) Background Screening

The responsible entity shall:

(i) Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s).

(ii) The responsible entity shall review the document referred to in section 1303.2.4.1 quarterly, and update the listing within two business days of any substantive change of personnel.

(iii) Access revocation must be completed within 24 hours for any personnel who have a change in status where they are not allowed access to critical cyber assets (e.g., termination, suspension, transfer, requiring escorted access, etc.).

(iv) The responsible entity shall conduct background screening of all personnel prior to being granted 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 Social Security Number verification 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.

(v) Adverse employment actions should be consistent with the responsible entity's legal and human resources practices for hiring and retention of employees or contractors.

(vi) Update screening shall be conducted at least every five years, or for cause.

(m) Regional Differences

None identified

(n) 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 for cause to assess performance.

(2) The responsible entity shall keep documents specified in section 1303.2.4 for three calendar years, and background screening documents for the duration of

employee employment. The compliance monitor shall keep audit records for three years, or as required by law.

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

- Document(s) for compliance, training, awareness and screening;
- Records of changes to access authorization lists verifying that changes were made within prescribed time frames;
- Supporting documentation (e.g., checklists, access request/authorization documents);
- Verification that quarterly and annual reviews have been conducted;
- Verification that personnel background checks are being conducted.

(o) Levels of Noncompliance

(1) Level One

(i) 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

(ii) One instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 2 business days; or

(iii) Background investigation program exists, but consistent selection criteria is not applied, or

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

(v) Awareness program exists, but not applied consistently or with the minimum of quarterly reinforcement.

(2) Level Two

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

(ii) 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 two business days; or

(iii) Training program exists, but doesn't not cover one of the specific items identified, or

(iv) Awareness program does not exist or is not implemented, or

(v) Background investigation program exists, but not all employees subject to screening have been screened.

(3) Level Three

(i) Access control list exists, but does not include service vendors; and contractors or

(ii) More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 2 business days; or

(iii) No personnel background screening conducted; or

(iv) Training documents exist, but do not cover two of the specified items.

(v) Level Four

(vi) Access control rights list does not exist; or

(vii) No training program exists addressing critical cyber assets.

(p) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1304 Electronic Security

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.

(a) Requirements

(1) 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.

(2) Electronic Access Controls:

The responsible entity shall implement the organizational, technical, and procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s). These controls shall implement an access control model that denies access by default unless explicit access permissions are specified. 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.

Electronic access control devices shall display an appropriate use banner upon interactive access attempts.

(3) 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.

(4) Documentation Review and Maintenance

The responsible entity shall ensure that all documentation reflect current configurations and processes. The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes.

(b) Measures

(1) 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 document or set of documents shall verify that all critical cyber assets are within the electronic security perimeter(s).

(2) Electronic Access Controls: 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). For each control, the document or set of documents shall identify and describe, at a minimum, the access request and authorization process implemented for that control, the authentication methods used, and a periodic review process for authorization rights, in accordance with management policies and controls defined in 1301, and on-going supporting documentation (e.g., access request and authorization documents, review checklists) verifying that these have been implemented.

(3) Monitoring Electronic Access Control: The responsible entity shall maintain a document identifying organizational, technical, and procedural controls, including tools and procedures, for monitoring electronic (logical) access. This document shall identify supporting documents, including access records and logs, to verify that the tools and procedures are functioning and being used as designed. Additionally, the document or set of documents shall identify and describe processes, procedures and technical controls and their supporting documents implemented to verify 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.

(4) Documentation Review and Maintenance: The responsible entity shall review and update the documents referenced in 1304.2.1, 1304.2.2, and 1304.2.3 at least annually or within 90 days of the modification of the network or controls.

(c) Regional Differences

None specified.

(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 document revisions and exception and other security event related data (such as unauthorized access reports) for three 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 days. 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:

(i) Document(s) for configuration, processes, tools, and procedures as described in 1304.2.1, 1304.2.2, 1304.2.3.

(ii) Records of electronic access to critical cyber assets (e.g., access logs, intrusion detection logs).

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

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

(e) Levels of Noncompliance

(1) Level One

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

Monitoring is in place, but a gap in the access records exists for less than seven days.

(2) Level Two

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

Access not monitored to any critical cyber asset for less than one day.

(3) Level Three

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

Electronic Access Controls:

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

Supporting documents exist, but not all transactions documented have records.

Electronic Access Monitoring:

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

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

(4) Level Four

No document or no monitoring of access exists.

(f) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1305 Physical Security

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) within which these assets reside. This standard requires:

- The identification of the physical security perimeter(s) and the development of an in-depth defense strategy to protect the physical perimeter within 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 physical access to the perimeter(s) and the critical cyber assets.

When physical perimeters are defined, different security levels shall be assigned to these perimeters depending on the assets within these perimeter(s).

(a) Requirements

(1) Documentation: The responsible entity shall document their implementation of the above requirements in their physical security plan.

(2) Physical Security Perimeter: The responsible entity shall identify in its physical security plan the physical security perimeter(s) surrounding its critical cyber asset(s) and all access points to the perimeter(s). Access points to the physical security perimeter(s) shall include all points of physical ingress or egress through the nearest physically secured “four wall boundary” surrounding the critical cyber asset(s).

(3) 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).

(4) 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.

(5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.

(6) Maintenance and testing: The responsible entity shall implement a comprehensive 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.

(b) Measures

(1) Documentation Review and Maintenance: The responsible entity shall review and update their physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods.

(2) 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).

(3) 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 card holder 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 Cage	A caged system that controls physical access to the critical cyber asset (for environments where the nearest four 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 each physical access point through the physical security perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and de-authorization process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in 1301, and on-going supporting documentation.

(4) 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.
Alarm Systems	An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include 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 identify and describe processes, procedures, and operational controls to verify access

records for authorized access against access control rights. The responsible entity shall have a process for creating unauthorized incident access reports.

(5) 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.
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.

(6) Maintenance and testing of physical security systems: The responsible entity shall maintain documentation of annual maintenance and testing for a period of one year.

(c) Regional Differences

None specified.

(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 document revisions and exception and other security event related data including unauthorized access reports for three calendar years. The compliance monitor shall keep audit records for 90 days.

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

(i) The Physical Security Plan

(ii) Document(s) for configuration, processes, tools, and procedures as described in 1305.2.1-6.

(iii) Records of physical access to critical cyber assets (e.g., manual access logs, automated access logs).

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

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

(e) Levels of Noncompliance

(1) Level One

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

(ii) Access control, monitoring and logging exists, but aggregate gaps over a calendar year in the access records exists for a total of less than seven days.

(2) Level Two

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

(ii) Access control, monitoring and logging exists, but aggregate gaps over a calendar year in the access records exists for a total of less than one month.

(3) Level Three

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

(ii) Access control, monitoring and logging exists, but aggregate gaps over a calendar year in the access records exists for a total of less than three months.

(4) Level Four

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

(f) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1306 Systems Security Management

The responsible entity shall establish a System Security Management Program that minimizes or prevents the risk of failure or compromise from misuse or malicious cyber activity. The minimum requirements for this program are outlined below.

(a) Requirements

(1) Test Procedures:

All new systems and significant changes to existing critical cyber security assets must use documented information security test procedures to augment functional test and acceptance procedures.

Significant changes include security patch installations, cumulative service packs, release 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 must be performed in a manner that precludes adversely affecting the production system and operation.

(2) Account and Password Management:

The responsible entity must establish an account password management program to provide for access authentication, audit ability of user activity, and minimize the risk to unauthorized system access by compromised account passwords. The responsible entity must establish end user account management practices, implemented, and documented that includes but is not limited to:

(i) Strong Passwords:

In the absence of more sophisticated methods, e.g., multi-factor access controls, accounts must have a strong password. For example, a password consisting of a combination of alpha, numeric, and special characters to the extent allowed by the existing environment. Passwords shall be changed periodically per a risk based frequency to reduce the risk of password cracking.

(ii) Generic Account Management

The responsible entity must have a process for managing factory default accounts, e.g., administrator or guest. The process should include the removal or renaming of these accounts where possible. For those accounts that must remain, passwords must be changed prior to putting any system into service. Where technically supported, individual accounts must be used (in contrast to a group account). Where individual accounts are not supported, the responsible entity must 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, and steps for securing the account in the event of staff changes, e.g., change in assignment or exit.

(iii) Access Reviews

A designated approver shall review 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 must be disabled.

(iv) Acceptable Use

The responsible entity must have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges. The policy must support the audit of all account usage to and individually named person, i.e., individually named user accounts, or, personal registration for any generic accounts in order to establish accountability of usage.

(3) Security Patch Management

A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets. Formal change control and configuration management processes must be used to document their implementation or the reason for not installing the patch. In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented.

(4) Integrity Software

A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter.

(5) Identification of Vulnerabilities and Responses

At a minimum, a vulnerability assessment shall be performed at least annually that includes a diagnostic review (controlled penetration testing) of the access points to the electronic security perimeter, scanning for open ports/services and modems, factory default accounts, and security patch and anti-virus version levels. The responsible entity will implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment.

(6) Retention of Systems Logs

All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) 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) years in an exportable format, for possible use in further event analysis.

(7) Change Control and Configuration Management

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.

(8) Disabling Unused Network Ports/Services

The responsible entity shall disable inherent and unused services.

(9) Dial-up modems

The responsible entity shall secure dial-up modem connections.

(10) Operating Status Monitoring Tools

Computer and communications systems used for operating critical infrastructure must include or be augmented with automated tools to monitor operating state, utilization, and performance, at a minimum.

(11) Back-up and Recovery

Information resident on computer systems used to manage critical electric infrastructure must be backed-up on a regular basis and the back-up moved to a remote facility. Archival information stored on computer media for a prolonged period of time must be tested at least annually to ensure that the information is recoverable.

(b) Measures

(1) Test Procedures

For all critical cyber assets, the responsible entity's change control documentation shall include corresponding records of test procedures, results, and acceptance of successful completion. Test procedures must also include full detail of the environment used on which the test was performed. The documentation shall verify that all changes to critical cyber assets were successfully tested for potential security vulnerabilities prior to being rolled into production, on a controlled non-production system.

(2) Account and Password Management

The responsible entity shall maintain a documented password policy and record of quarterly 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. Upon normal movement of personnel out of the organization, management must review access permissions within 5 working days. For involuntary terminations, management must review access permissions within no more than 24 hours.

(3) 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, management approval for installation, and installation date. The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels. The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability.

(4) Integrity Software

The responsible entity's critical cyber asset inventory and change control documentation shall include a record of all anti-virus, anti-Trojan, and other system integrity tools employed, and the version level actively in use. The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available updates to these tools security patches/OS upgrades and current revision/patch levels. The documentation shall verify that all critical cyber assets are being kept up to date on available integrity software so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware. Where integrity software is not available for a particular computer platform or other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malware must also be documented.

(5) Identification of Vulnerabilities and Responses

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. The documentation will also include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. The documentation shall verify that the responsible entity is taking appropriate action to address the potential vulnerabilities.

(6) Retention of Logs

The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. 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.

(7) 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.

(8) Disabling Unused Network Services/Ports
The responsible entity shall maintain documentation of status/configuration of network services and ports on critical cyber assets, and a record of the regular audit of all network services and ports against the policy and documented configuration. The documentation shall verify that the responsible entity has taken the appropriate actions to secure electronic access points to all critical cyber assets.

(9) Dial-up Modems

The responsible entity shall maintain a documented policy for securing dial-up modem connections to critical cyber assets, and a record of the regular audit of all dial-up modem connections and ports against the policy and documented configuration. The documentation shall verify that the responsible entity has taken the appropriate actions to secure dial-up access to all critical cyber assets.

(10) Operating Status Monitoring Tools

The responsible entity shall maintain a documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of critical cyber assets.

(11) Back-up and Recovery

The responsible entity shall maintain a documentation that index location, content, and retention schedule of all backup data and tapes. 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. The documentation shall verify that the responsible entity is capable of recovering from the failure or compromise of critical cyber asset.

(c) Regional Differences

None

(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:

(i) Document(s) for configuration, processes, tools and procedures as described in 1306.2.1, 1306.2.2, 1306.2.3, 1306.2.4, 1306.2.8, and 1306.2.9.

(ii) System log files as described in 1306.2.6.

(iii) 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.).

(e) Levels of Noncompliance

(1) Level one:

(i) Document(s) exist, but have does not cover up to two of the specific items identified and/or

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

(2) Level two:

(i) Document(s) exist, but does not have three of the specific items identified and/or

(ii) A gap in the monthly/quarterly reviews for the following items exists:

A) Account and Password Management (quarterly)

B) Security Patch Management (monthly)

C) Anti-virus Software (Monthly)

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

(3) Level three:

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

(ii) Test Procedures: Document(s) exist, but documentation verifying that changes to critical cyber assets were not tested in scope with the change.

(iii) Password Management:

A) Document(s) exist, but documentation verifying accounts and passwords comply with the policy does not exist and/or

B) 5.3.3.2 Quarterly audits were not performed.

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

(v) Integrity Software: Documentation exists, but verification that all critical cyber assets are being kept up to date on anti-virus software does not exist.

(vi) Identification of Vulnerabilities and Responses:

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

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

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

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

(ix) Change Control and Configuration Management: N/A

(x) Operating Status Monitoring Tools: N/A

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

(4) Level four:

No document exists.

(f) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1307 Incident Response Planning

Security measures designed to protect critical cyber assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis. Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified.

(a) Requirements

(1) The responsible entity shall develop and document an incident response plan. The plan shall provide and support a capability for reporting and responding to physical and cyber security incidents to eliminate and/or minimize impacts to the organization. The incident response plan must address the following items:

(2) Incident Classification: The responsible entity shall define procedures to characterize and classify events (both electronic and physical) as either incidents or cyber security incidents.

(3) Electronic and Physical 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.

(4) Incident and Cyber Security Incident Reporting: The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP).

(b) Measures

(5) The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements.

(6) The responsible entity shall retain records of incidents and cyber security incidents for three calendar years.

(7) The responsible entity shall retain records of incidents reported to ESISAC for three calendar years.

(b) Regional Differences

None specified.

(c) 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 all records related to incidents and cyber security incidents for three calendar years. This includes, but is not limited to the following:

(i) System and application log file entries related to the incident,

(ii) Video, and/or physical access records related to the incident,

(iii) Documented records of investigations and analysis performed,

(iv) Records of any action taken including any recovery actions initiated.

(v) Records of all reportable incidents and subsequent reports submitted to the ES-ISAC.

(3) The responsible entity shall make all records and documentation available for inspection by the compliance monitor upon request.

(4) The compliance monitor shall keep audit records for three years

(d) Levels of Noncompliance

(1) Level One

(i) Documentation exists, but has not been updated with known changes within the 90-day period and/or

(2) Level Two

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

(ii) Records related to reportable security incidents are not maintained for three years or are incomplete.

(3) Level Three

(i) Incident response documentation exists but is incomplete

(ii) There have been no documented cyber security incidents reported to the ESISAC.

(4) Level Four

No documentation exists.

(e) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.

1308 Recovery Plans

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function must establish recovery plans and put in place the physical and cyber assets necessary to put these recovery plans into effect once triggered. Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices.

The recovery plans and the physical and cyber assets in place to support them must be exercised or drilled periodically to ensure their continued effectiveness. The periodicity of drills must be consistent with the duration, severity, and probability associated with each type of event. For example, a higher probability event with a short duration may not require a recovery plan drill at all because the entity exercises its response regularly. However, the recovery plan for a lower probability event with severe consequences must have a drill associated with it that is conducted, at minimum, annually.

Facilities and infrastructure that are numerous and distributed, such as substations, may not require an individual Recovery Plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area and this will require a redundant or backup facility. Because of these differences, the recovery plans associated with control centers will differ from those associated with power plants and substations. There is no requirement for recovery plans for substations and generation plants that have no critical cyber assets.

(a) Requirements

(1) The responsible entity shall create recovery plans for critical cyber assets and exercise its recovery plans at least annually.

(2) The responsible entity shall specify the appropriate response to events of varying duration and severity that would trigger its recovery plans.

(3) The responsible entity shall update its recovery plans within 30 days of system or procedural change as necessary and post its recovery plan contact information.

(4) The responsible entity shall develop training on its recovery plans that will be included in the security training and education program.

(b) Measures

(1) The responsible entity shall document its recovery plans and maintain records of all exercises or drills for at least three years.

(2) The responsible entity shall review and adjust its response to events of varying duration and severity annually or as necessary.

(3) The responsible entity shall review, update, document, and post changes to its recovery plans within 30 days of system or procedural change as necessary.

(4) The responsible entity shall conduct and keep attendance records to its recovery plans training at least once every three years or as necessary.

(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 1308.2.1. through 1308.2.4. available for inspection by the compliance monitor upon request.

(e) Levels of Noncompliance

(1) Level one: Recovery plans exist, but have not been reviewed or updated in the last year. Exercises, contact lists, posting, and training have been performed adequately.

(2) Level two: Recovery plans have not been reviewed, exercised, or training performed appropriately.

(3) Level three: Recovery plans do not address the types of events that are necessary nor any specific roles and responsibilities.

(4) Level four: No recovery plans exist.

(f) Sanctions

Sanctions shall be applied consistent with the NERC compliance and enforcement matrix.